

**Digimarc Testimony for Border Security:
Center for Strategic and International Studies**

Scott Carr, Executive Vice President
Digimarc Corporation
9405 SW Gemini Drive
Beaverton, OR 97008 USA
Tel: +1 800 DIGIMARC (344 4627)

Executive Summary

Digimarc is the leading supplier of government-issued citizen identity documents in North America. Our systems are used to enroll citizens and issue more than two-thirds of all U.S. driver licenses. We supply similar systems for production of the Mexican voter identification document and driver licenses in several Canadian provinces.

Customs and Border Protection and law enforcement officers face extraordinary challenges as they try to authenticate the more than 200 forms of valid driver licenses circulating in the U.S. today through unaided visual inspection. This paper discusses the security innovations being made by several State governments as they enhance the security of driver licenses and move to comply with the REAL ID Act. Further, this paper addresses the technological innovations that are available now and in use by several State governments and commercial entities to augment visual inspection of driver licenses. Such technologies, like digital watermarking, are already in broad distribution, and can be used to machine authenticate U.S. driver licenses, travel documents and other modern identification documents. Solutions, like those discussed today, could be leveraged by the U.S. Federal government to improve the security of our borders within 6 to 12 months. The option of incorporating a micro-chip in driver licenses is also discussed as an alternative approach to enable the government to achieve the objectives of the Western Hemisphere Travel Initiative (WHTI) and the PASS program, a set of new requirements for travel documents.

Although many States are engaging in impressive innovation in driver license security, we will pay special attention today to a Department of Transportation pilot study conducted by Nebraska that is right on point with the concerns of the Committee. This pilot study, coupled with the investments that Nebraska has made in identification security, provides a useful case study to inform the national debate about the use of driver licenses for crossing our land borders with neighboring nations. A demonstration of readily available solutions that can machine validate identification documents is

provided, as are a number of public policy recommendations that seek to contribute to implementing effective strategies to protect our homeland.

Introduction

I would like to thank the Center for Strategic and International Studies for giving me an opportunity to take part in this important conference. Digimarc Corporation welcomes the opportunity to offer its expertise in ID security to both the business community and the government to help develop a solution that will protect our border and help ensure that commerce continues to prosper across the U.S., Canadian, and Mexican borders.

I am appearing at today's conference as an expert in the field of secure ID solutions. As an Executive Vice President at Digimarc Corporation, I have responsibility for business development and managing our North America customer relationships for Digimarc's secure identification solutions. In my 10 years with Digimarc, I have held a number of executive management positions leading the development and successful deployment of digital watermarking and government-oriented document and ID security applications.

Digimarc Overview

Digimarc has been in the business of supplying issuance systems for driver licenses and other government-issued credentials for nearly 50 years. Our company is the leading supplier of government-issued IDs in North America and also supplies similar products and services in more than 20 foreign countries including Mexico, Haiti, Russia and the United Kingdom. We are also a trusted supplier of a global system used by an international consortium of central banks to deter digital counterfeiting of banknotes.

Our company's systems issue more than 60 million identification documents annually, and are employed by 32 U.S. States and the District of Columbia, producing more than two-thirds of all driver licenses issued. We support the States with solutions that cover all aspects of ID issuance, including applicant identity verification and enrollment, over-the-counter and centralized secure card production systems, design and manufacturing of the cards using advanced technologies and multiple security features, and inspection to authenticate the ID after it has been issued. To date, Digimarc provides centrally issued driver licenses to 12 States, comprising approximately 80% of all centrally issued IDs in the U.S.

Additionally, Digimarc has pioneered a signal processing technology innovation known as "digital watermarking," which allows imperceptible digital information to be

embedded in all forms of media content, including personal identification documents, financial instruments, photographs, movies, music and product packages. In identity documents digital watermarking is used to embed digital data within the structure of the document that is imperceptible to the human eye. It creates a machine-readable security feature that links together numerous elements of the document allowing machine authentication to readily identify counterfeit and fraudulent documents.

At the point of inspection, digital watermarks can be easily detected and read by a number of commercially available devices, including document scanners, PDAs with built-in cameras, mobile phones and other digital devices. A quick scan by an authorized reading device, equipped with special software, analyzes the information embedded in the digital watermark as well as other information contained in security features present on the document. This enables the immediate detection of photo swapping, altered data or re-originated documents -- the primary forms of counterfeiting.

U.S. States began incorporating digital watermarking in their driver licenses in 2002 using a Digimarc product known as Digimarc® IDMarc™. Twenty States have adopted this important security capability in their driver licenses, including key border States such as Washington, Michigan, Minnesota, Florida, Texas, and Vermont. In Michigan, for example, more than 75% of circulating licenses contain a digital watermark that could be authenticated at the U.S. / Canadian border. Examples of States in other areas of the country that have adopted digital watermarking include Iowa, Wyoming, Nebraska, New Jersey, Kansas, and Massachusetts.

By the end of 2006 more than 50 million circulating driver licenses will include digital watermarking. This security feature is not perceptible on the document, but is easily read with a scanner and proprietary software, enabling reliable cross-jurisdictional authentication of U.S. driver licenses. In 2007 Digimarc anticipates that 1 in every 2 issued driver licenses will include digital watermarks and this number is growing rapidly.

Digital watermarking complements other authentication techniques such as the pattern matching and multi-spectral analyses found in passport and travel document scanners. Digital watermarking technology is compatible with and can enhance the security of passports, smartcards and other travel documents such as the proposed PASS Card. Digimarc broadly licenses digital watermarking technologies to many other vendors for supply of digital watermarking enhanced solutions for a variety of security purposes.

Deployment of digital watermark reading is aligned with the published security strategies of the Department of Homeland Security and the Department of State, and is a

recommended feature of the Document Security Alliance and an approved optional feature of the HSPD-12 PIV-2 standard, which calls for enhancing the identification and authentication of federal employees and contractors. Digital watermarks provide positive document authentication, age verification, cross-jurisdictional authentication, and forensic capabilities.

The Economic Challenges of the PASS Card

The Intelligence Reform and Terrorism Prevention Act was signed into law in December 2004. A provision included in that Act, the Western Hemisphere Travel Initiative (WHTI), set new requirements for travel documents that take effect, under an implementation schedule that had initially been announced by the Bush Administration to take effect in January 2008. Congress delayed implementation of this Act by 18 months to give the Administration more time to develop a technical implementation plan. Congress was also urged to pass this delay by Canadian and US business interests who fear that the original PASS program could reduce commerce between the two countries.

WHTI mandates that upon seeking entrance to the United States across a land border port of entry, all travelers, including U.S. citizens, present a passport, another verifiable and secure document, or combination of documents which can ensure a person's identity and citizenship. This initiative will change travel for U.S. citizens traveling between the U.S. and both Canada and Mexico.

More than 29 million people move across the U.S. / Canadian border to engage in trade and tourism each year, supporting more than \$1.2 billion of daily trade between the countries. In 2004, Canadians spent \$10.3B in the U.S., nearly \$8 billion of which was spent on travel and tourism.

Only 25% of U.S. Citizens hold passports. The initial implication of WHTI was that each citizen traveling home from Canada or Mexico would now have to possess a valid passport, costing nearly \$100 to obtain. To ease the financial burden, and to partly address the concerns of the business community, the Department of Homeland Security, the agency with authority over this Act, has proposed a driver-license-like "passport lite" document called the PASS Card. However, Zogby International has released a poll that found that 68 percent of Americans and 54 percent of Canadians are unlikely to purchase an additional, limited use government issued card.

The PASS Card proposal duplicates many of the requirements of The REAL ID Act, which was signed into law in 2005. This Act calls for new standards in driver licenses, and mandates that only compliant driver licenses can be used for Federal purposes. Upon implementation of the REAL ID Act by States in May 2008, the U.S. driver license, which currently acts as the gateway document to social services and privileges, will be even more secure than it is today. The processes used to issue a REAL ID driver license will be even more reliable than many Federal ID programs and are ideal to carry out the enrollment process for PASS Cards.

A coalition of U.S. and Canadian businesses, called Business for Economic Security, Trade & Tourism (BESTT) and comprised of over 60 associations and companies, believes that the PASS proposal, as currently written, will significantly reduce commerce between the US and Canada. Indeed, BESTT has cited one estimate saying the new identification requirements could cost the U.S. economy \$785 million a year and the Canadian economy \$1.7 billion in lost revenue due to a decline in tourism. This coalition “opposes requiring passports for Americans and Canadians entering the US, and instead, urges the US and Canadian government to develop another approach that would do a better job of balancing commercial and homeland security interests. The coalition has also urged both the US and Canadian government to consider allowing Real ID compliant drivers licenses to be used as border crossing cards.

Leveraging State Investments in ID Security to Secure our Borders

States have made and are making major investments in their driver licenses and issuance systems to promote transportation safety, protect their citizens from identity theft and fraud, and enhance the personal security and the security of the nation. As we know, the perpetrators in the Sept. 11 terrorist attacks obtained valid driver licenses under false identities. In any security system, criminals tend to look for weak points to exploit. In these cases, the documents were genuine driver licenses obtained fraudulently. The States and their suppliers are upgrading not only the documents but also the enrollment process and inspection processes to address all know weaknesses that could be exploited by criminals. According to the National Conference of State Legislatures, the States are expecting to invest \$11 billion as they continue to enhance the security of their driver licenses in compliance with federal standards being established to implement the REAL ID Act. These efforts will result in a citizen ID infrastructure that will deliver a high level of security in the enrollment, issuance and inspection processes. The States have established security processes that complement and extend many of the steps that are used for the current passport, or expected PASS card.

The processes and technologies being deployed by the States create a widespread enrollment and issuance infrastructure that could also be used to strengthen the enrollment processes for citizen credentials such as Passports, and can be used in conjunction with gaining citizenship certification from Department of State for State-issued REAL ID-compliant driver licenses. These improved enrollment processes include:

- Secure in-person photo capture to protect against fraudulent photo submittal and enable downstream biometric facial recognition

- Electronic scanning and archiving of documents enabling efficient enrollment, subsequent forensic investigation of documents, and electronic transmittal as part of adjudication process
- Electronic document authentication at point of enrollment using a variety of machine readable features including digital watermarking
- Electronic applicant verification against federal and third party databases such as Social Security
- Electronic verification of applicant data against State DMV and vital record databases
- Facial and/or fingerprint recognition, both 1-to-1 and 1-to-many, to verify identity against existing biometric records
- Use of trained driver license agency personnel who are experienced in fraudulent document recognition, work with enrollment processes on an ongoing basis, and have successfully passed thorough background checks

Leveraging Existing Technologies to Secure our Borders

As described above, proven, cost-effective technologies are commercially available today that can enable border officials to machine authenticate U.S. driver licenses. These documents contain numerous security features such as digital watermarks, holograms, and special inks. There are software and hardware solutions available that can automatically inspect such security features and facilitate background checks via third party data bases. Digital watermarks are key in that they provide the only means in use today of trusted authentication of a driver license, and can be read using commercially available scanners and special software.

In addition to applicability in detecting and deterring ID counterfeiting, digital watermarks are a proven layer of security in global efforts to protect banknotes from digital counterfeiting. We have a multi-year contract with an international consortium of Central Banks in which we have developed and deployed, and are supporting and continuing to enhance a system to deter digital counterfeiting of currency using personal computers and digital reprographics. Work on the system began in 1997. Further details of the system are confidential for security reasons, yet it is important to note that digital watermarking is a proven and widely deployed security technology in such other anti-counterfeiting initiatives.

Digital watermark-based document authentication solutions are compatible with other travel document reading efforts, including the ePassport efforts. This capacity to work with an ever-evolving set of security features is essential because it ensures that our government can stay ahead of terrorists and criminals who seek to use loopholes in our

security systems to gain access to our country. Additionally, these technologies can be quickly deployed, within 6 to 12 months, and are efficient for the inspector to use so that citizens are not inconvenienced with long lines. And essential to success, digital watermarks do not compromise citizen privacy.

Summary of Nebraska ID Authentication Pilot Results

We would like to discuss what one State, Nebraska, has already done to raise the ID security bar by deploying innovative security solutions and processes. The experience of Nebraska, and similar experiences in several other States that have implemented driver license security innovations, can be leveraged by the Federal government to help make our nation's borders more secure in a timely and cost effective way. Iowa, for instance, has deployed secure card materials, digital watermarking, and many other cutting edge solutions. The State employs fulltime investigators to attack license and identity fraud, and has deployed advanced readers to help officials detect counterfeits.

Today, more than 60% of valid driver licenses in Nebraska are secured with digital watermarking, and Digimarc anticipates within two years all valid Nebraska licenses in circulation will be protected by IDMarc.

In 2005, the Nebraska Department of Motor Vehicles conducted a pilot under a grant from the U.S. Department of Transportation to demonstrate authentication of digitally watermarked driver licenses as a means to fight ID counterfeiting, reduce the purchase of age-restricted products, such as alcohol, and enhance traffic safety.

Digital watermark scanners were installed in a total of 18 point-of-sale sites, 30 office sites, and 35 law enforcement sites, and were used in "real time" for an average of 30 days. The deployed readers continue to be used by the state, and in fact, this summer, Nebraska plans to put new Digimarc Document Inspector units into production at DMVs across the State. This will arm front-office operators with the tools to inspect and positively authenticate the millions of U.S. driver licenses secured with Digimarc IDMarc digital watermarking. Authentication will take place when Nebraska and other State driver licenses are presented as proof of identity to obtain a new or renewal driver license. This includes licenses from neighboring States such as Colorado, Iowa, Kansas and Wyoming - effectively removing the guesswork that can come with visually inspecting an out-of-state ID.

At the conclusion of the pilot, Digimarc staff interviewed the users regarding their experience with and response to the digital watermarking technology. Retailers, law

enforcement and DMV operators were equipped with reader devices that allowed them to verify the information printed on a driver license -- even an unfamiliar out-of-state driver license -- against the information contained in the digital watermark. By doing so, they were able to determine if a driver license was valid or not and in the retail situations which, if any, age-controlled products the driver license holder was old enough to purchase. The scanner/reader devices proved invaluable in instantly determining whether or not the license presented was authentic, as well as validating the age of the driver license holder.

- 100% of retail participants said that a valid read from the watermark gave them confidence that the driver license was authentic.
- 100% of law enforcement participants using a PDA reading device had confidence that a valid read from the watermark meant the driver license was authentic.

100% of office staff surveyed reported that they believed the device was beneficial, that it gave them confidence that the scanned ID was authentic, and that they would use it in the future.

Digimarc Document Inspector Scenario

Authenticating documents like driver licenses and IDs can be done quickly and simply with a single device that scans both sides of the document simultaneously, and the Digimarc Document Inspector software that checks the validity of common ID security features, including the digital watermark.

Given a driver license, to determine if it is genuine, an inspector would start inspecting the document by inserting it into the scanner. The software is very easy to use -- the operator just hits the spacebar to initiate the scanning process.

In just a few seconds, the device scans both sides of the document and the software processes the information, determining if the document is authentic for that document type and jurisdiction. The software contains a regularly updated document information library that is used for this automated validation process.

The software read the individual's demographic data from the document to display to the operator, which assists validation of the document and card holder. This entire process produces a valid rating in seconds, displaying "green" clearly on the screen so it's easy for the operator to see it passed inspection - enabling them to focus on the individual, rather than the document.

The scanning process of a counterfeit or altered document is the same, only the result is a clear red indicator on the screen that the document is suspect. This counterfeit might have been made by swapping a photograph from a driver license produced in a different State, and placing it on a valid license. The software is able to determine the mismatch and flag the document as suspicious for the operator to take action or conduct further investigation. In a typical border crossing scenario, this card holder would be sent to secondary inspection where an investigator could use the digital watermark and other features or databases to pursue the fraud.

Digital watermarks can also be read and authenticated on travel document scanners, like the kind used to read passports. Our software is able to draw on the pattern matching library of such a scanner and its multi-spectral light inspection authenticate the watermark and check additional security features visible only when illuminated in UV or IR light. This is a more expensive solution, but one that can validate not just driver licenses and IDs, but travel documents like passports and foreign ID cards.

The Digimarc Document Inspector closes the loop on the secure ID lifecycle by providing an easy, reliable way to instantly authenticate IDs after issuance. Border inspectors can immediately validate the document using the digital watermark and other data and features present on the license. Visible features, like 2D barcodes and others, can be altered, but when linked to a second feature that is imperceptible to the human eye, counterfeiting becomes extremely difficult, if not impossible. After scanning, Document Inspector provides a quick pass/fail reading and keeps lines moving.

Digimarc Document Inspector is fast and easy-to-use. An operator can authenticate a document with confidence in just a few seconds. Our software is hardware independent, working seamlessly with a variety of best-of-breed hardware and software components, and provides a simple user interface to eliminate the guess work associated with visual inspection.

Document Inspector can validate a deep set of security features. Depending on options selected this includes an extensive database of U.S. driver license security features such as barcodes, magnetic stripes, document layout features in visible light (placement, size), and features in UV and IR light. The database is updated on a regular basis, and updates can be distributed in multiple ways.

Table 1 summarizes the Document Inspector features and benefits.

Table 1 Digimarc Document Inspector Features and Benefits

| Features | Benefits |
|---|--|
| Extensive document database that is updated regularly | <ul style="list-style-type: none"> • Standardizes authentication practices • Gives agents more confidence • Keeps the knowledge base up to date without the need for additional training |
| Fast, easy authentication results | <ul style="list-style-type: none"> • A clear red/green indicator of authentication evaluation • Multiple visual cues to the result • Ability to see the details if further investigation is necessary |
| Standards-based technology | <ul style="list-style-type: none"> • Allows for integration with external systems • Keeps deployment/investment costs low • Provides clear technology path |

In summary Digimarc Document Inspector is a document authentication solution that features:

- A system that offers fast document authentication to ensure citizens are not inconvenienced or slowed down by the process.
- Authentication of the most comprehensive set of security features used in driver licenses

Cost Estimates of Deploying Readily Available Technologies

Digimarc does not have access to all of the government information, including technology integration, human resource, and third-party database expenses, to offer a precise estimate of what it would cost the Federal government to deploy these readily available technologies to help secure our borders. We respectfully suggest that the Committee request that the Congressional Budget Office or the Office of Management and Budget conduct such a study.

It is our understanding that the number of Northern and Southern land border points of entry are:

| | Inbound Passenger Lanes | Inbound Cargo Lanes | Pedestrian Lanes | Total Lanes |
|---------------------------|-------------------------|---------------------|------------------|-------------|
| Northern Land Border POEs | 278 | 121 | 24 | 423 |
| Southern Land Border POEs | 224 | 72 | 86 | 382 |
| Total | 502 | 193 | 110 | 805 |

Our own rough estimate of the cost -- based on our experience and market research studies -- of deploying the necessary software and hardware in an estimated 805 lanes to cover all immigration land border lanes, including cargo and shoulder lanes is under \$50 million. This would equip each lane to machine validate driver licenses and other common travel documents. Covering the Northern border lanes, assuming 423, the cost is approximately \$26 million. If we wanted to add any type of remote database interface to this system such as cross referencing watch list databases or consolidating the number of transactions etc. we would add an additional \$10 million to our baseline cost estimates.

These cost estimates do not include the cost to the States of deploying machine-readable security features, nor do they capture the expense to the States of improving a large number of their security programs such as their enrollment processes. But these requirements have already been mandated by the REAL ID Act and the States are already working out how to pay for compliance with this Act. In any case, if our cost estimates are roughly in the ball park, this would be a small price to pay to quickly improve the security of our borders.

New Technologies: A Smart Card Capability to Enhance the Security of Travel Documents

Although the Federal government could leverage the current investments the state have made and will make in ID security to enhance the safety of border travel, it has remained committed to bringing the PASS card on line. One key component of the government plan is to include a micro-chip in this card to enable it to either run on the same technology infrastructure of the new Passport that is being rolled out, or to introduce a remote reading capability – the ability to determine a few minutes before citizens actually

cross the border whether their credentials are valid. This capability, the government believes, will help ensure that citizens can move quickly across the border while ensuring that high level of security is maintained.

Digimarc recently announced that its proven driver license solution is now available with a contactless smart card option. Digimarc provides driver license issuers an advanced and proven centrally issued driver license solution that can now incorporate a range of contactless smart card technologies. Digimarc's smart card-enabled driver license solution also gives the Federal government an attractive, alternative means to meet its "PASS" card objectives with a low-risk, low-cost solution that leverages existing State ID issuance infrastructures.

Digimarc's smart card option for secure driver licenses keeps pace with emerging technologies and is responsive to States and Canadian provinces that want to maintain use of the driver license as an acceptable form of identification for border crossing. This new driver license solution is designed to give citizens a convenient and cost-effective alternative to the use of a passport or special 'PASS' card for border crossing. Use of the new driver license solution for border crossing is subject to Federal government approval, which is being pursued by a number of States, members of Congress, and citizen advocacy groups.

Public Policy Recommendations

We recommend that the Federal government promptly deploy capabilities to machine verify the authenticity of U.S. driver licenses at the border, including reading and authenticating the digital watermark. Over time, these readers could be upgraded to accommodate enhancements being made to driver licenses and other identity documents from both the U.S. and Canada, and also other from other Western Hemisphere countries as deemed appropriate by the Department of Homeland Security and the Department of State. These technology solutions are scalable, having the capacity to integrate new technologies that will be developed in the future to ensure that criminals and terrorists are always challenged to defeat ever higher levels of security.

Every border crossing official must be able to do machine-readable verification of driver licenses, processing the covert machine readable features in documents that are presented at the border. In addition to putting stationary readers at all border crossing stations, mobile readers should also be deployed to ensure that agents can do rapid and secure screening of driver licenses and/or travel documents. This will help ensure that transit times are not unduly affected.

All of these technologies exist today and are proven, and could be deployed in 6 to 12 months if the funds were available. Even if the U.S. government implements new border crossing mandates in the future so that only passports are to be utilized for border crossing, a position which we disagree with as described below, such a deployment would provide additional security before that date and also could ensure the integrity of the proposed PASS cards.

The REAL ID law requires the States to add a machine-readable feature to their driver licenses. Given that digital watermarking has become a de facto standard for driver license authentication, we recommend that the Federal government require or encourage all States to adopt digital watermarking technology in addition to other appropriate machine-readable security features to comply with the requirements of this law so that national standard authentication will be realized.

We likewise urge Congress to help the States pay for REAL ID compliance. The REAL ID Act will help States meet the security challenges of the 21st century by ensuring that they deploy best-of-breed, end-to-end security systems. Given the cost-initial cost estimates by the National Conference of State Legislatures suggest that compliance will run between \$9 and \$13 billion--the Federal government should not impose a large unfunded mandate on the States to meet our national objective of protecting our homeland.

Finally, we recommend that Congress harmonize the Western Hemisphere Travel Initiative and the REAL ID Law. After two years of debate, the State Department and the Department of Homeland Security continue to grapple with the development of technical specifications for the proposed PASS card that is designed to implement WHTI without crippling cross-border commerce. In light of concerns with the ability of the government to have the structures in place to implement WHTI at the end of next year, we applaud the US government for having recently extended the implementation deadline of the PASS program by 18 months. Given the uncertainty associated with the PASS program we advocate that Congress insist that willing States be allowed to issue REAL-ID compliant driver licenses that would be an alternative to the PASS card for WHTI compliance.

This approach would leverage the significant investments in ID security that the States have already, and will continue to make, in the coming years, and would require DHS to establish a common standard of technical standards to be applied to any credential used for land border crossing. This approach would also leverage the existing ID systems that

the Canadian Provinces have already deployed. The opportunity for both the United States and Canada to develop a collaborative approach should not be missed.

Conclusion

In conclusion, I would like to thank CSIS for giving me the opportunity to speak at this conference. The States have been pressing forward with important security upgrades within the limits of their budgets and mandates. More will need to be done as States drive to comply with the REAL ID law. It makes sense, therefore, for the Federal government to leverage these significant investments to help secure our borders, and at the same time, save tax payers money and time in obtaining identification credentials. Digimarc Corporation, along with other suppliers and the many of the issuers that we serve stand ready to do all we can to support the government's objective of enhancing the security of our homeland.