



# BITS

FINANCIAL SERVICES  
R O U N D T A B L E

May 8, 2007

Department of Homeland Security  
Attn: NAC 1-12037  
DHS Docket Number: 2006-0030  
Washington, DC 20528

Subject: Comments on NPRM on Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes

Dear Sir/Madam:

The Financial Services Roundtable (Roundtable) and BITS, on behalf of our member companies, appreciate the opportunity to comment on the Department of Homeland Security's Notice of Proposed Rule Making (NPRM) that outlines the minimum standards for state-issued driver's licenses and identification cards in compliance with the REAL ID Act of 2005.

The Financial Services Roundtable is a national association that represents 100 of the largest integrated financial services companies providing banking, insurance, investment products, and other financial services to American consumers. Roundtable member companies provide fuel for America's economic engine, accounting directly for \$65.8 trillion in managed assets, \$1 trillion in revenue, and 2.4 million jobs.

BITS is a division of the Roundtable, leveraging intellectual capital to address issues at the intersection of financial services, operations and technology. BITS focuses on strategic issues where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services.

We would like to comment on the following five areas of concern, as identified by our members:

1. The importance of secure credentials to the financial services industry;
2. The operation of the "federated query service" and its protection of sensitive personal information;
3. The use and challenges associated with card encryption;
4. The security and protection of data and databases that house the personal information of consumers; and
5. The use of background checks on DMV employees.

Our member companies have extensive expertise in the processes and technologies needed to verify and authenticate customers and we welcome the opportunity to work collaboratively to develop a system that will safeguard the safety and integrity of our customers' information.

### **Importance of Secure Credentials to the Financial Services Industry**

The proposal establishes minimum standards for state-issued driver's licenses and identification cards that Federal agencies would accept for official purposes, such as boarding Federally-regulated aircraft and entering Federal facilities. These standards also will impact financial institutions because financial institutions rely on government-issued credentials such as driver's licenses to verify identity for everyday functions such as opening customer accounts, establishing loans, and hiring employees. In addition, financial institutions are required by government regulations to identify their clients and gather relevant information before doing business with them. Therefore, it is extremely important that when issuing IDs under this proposal, states take all steps necessary to verify both the identity of the individual and the authenticity of the documents presented to them.

Our members applaud efforts to improve the reliability and functionality of credentials such as state driver's licenses and state-issued identification cards. However, the proposal does not adequately address the importance of the enrollment process for issuing a driver's license or identification card. Unless the enrollment process is adequately addressed, the value to society of an expensive, new, state-based ID system using common standards and more advanced technology will be minimal. We urge the Department of Homeland Security (DHS) to work with industry and state governments to develop a proposal that includes a robust and trusted enrollment process to avoid situations where a fraudster or terrorist can acquire an ID under this proposal by presenting false documentation or exploiting a weak process.

In addition, this proposal provides an important opportunity to improve financial institutions' ability to "know their customer" as mandated by the USA Patriot Act and other laws and regulations. The proposal also highlights the industry's need to verify the authenticity of government-issued credentials and thus trust them. We believe it is crucial to take this opportunity to make available to the financial services industry a secure, reliable, and cost effective mechanism to verify state-issued driver's licenses and identification cards.

States have long had the ability to verify license information among themselves through American Association of Motor Vehicle Administrations' sponsored systems (AAMVA). Financial institutions have been left relying on the "appearance" of the driver's license or algorithmic systems that verify if a license has been issued and when to determine the possibility it belongs to a specific person (i.e., by age metrics). It is now time to extend our ability to protect the financial system from misuse by terrorists, identity thieves and others by making real-time verification of these critical identity documents available to the financial services industry. We urge DHS to quickly assess AAMVA's sponsored systems and either adopt these systems or begin to investigate the development of an alternative.

### **Federated Query Service**

The proposal states that DHS is committed to supporting the development of a "federated querying service" that will enable the states to access the Federal reference databases in a timely, secure, and cost-effective manner and that DHS is committed to expediting the development and deployment of a common voluntary querying service to facilitate the state DMV queries for REAL ID data verification. Most states already query some reference databases, either directly or indirectly, through a portal provided by AAMVA. It is not clear whether this will be the federated database of choice. If so, there is no reference as to what measures or standards will be used to enhance this system to accommodate the increase in inquiries and protect the consumer data.

### **Card Encryption**

DHS should urge states to develop and deploy a practical and cost-effective encryption standard, taking into account the many challenges with the encryption of data in storage and transit.

DHS should not urge encryption of the 2D bar code data unless it intends to make this information accessible to financial institutions and other parties that may have a legitimate need to access the information. In the case of financial institutions, this need is tied to the regulatory requirement that institutions know their customers. Many financial institutions currently have magnetic stripe readers, bar code scanners or other machine-readable devices for use with their respective state's driver's licenses. The information contained within the machine-readable section of the license contains nothing more than an electronic image of the information contained on the face of the license. In the absence of requiring information beyond the scope of the current configuration in the machine-readable section, encryption would be of little value since the information on the driver's license face is available for anyone in possession of the license to view, copy, write down, etc. States should be encouraged by DHS to establish a "common standard" for embedding driver's license and ID card information in the recommended 2D bar code to simplify its commercial use. DHS also should take into account the impact that a common standard will have on key management. If encryption is implemented, a jurisdictionally-varied approach should be taken. Sharing a single key across the nation could expose a substantial amount of personal data to a security breach. Robust key management systems are still rare in large enterprises. We believe that DHS should study the issue thoroughly and engage the financial services industry and other stakeholders before reaching conclusions on encryption and key management.

### **Data Protection**

The proposal states that "each state will be required to prepare a comprehensive security plan for its DMV offices and driver's license storage and production facilities, databases, and systems utilized for collecting, disseminating or storing information used in the issuance of REAL ID licenses." While DHS will require that each state include information in its annual certification as to how the state will protect the privacy of the data collected, used, and maintained in connection with REAL ID, including all the source documents, it does not state how these plans will be reviewed or audited and to what standards or measures these plans will be held.

The Act requires the data elements such as full legal name, date of birth, etc. to appear on recognized driver's licenses and state-issued ID cards. However, some states' data breach standards specifically define the date of birth as personal information warranting an elevated level of protection. Therefore, it seems inconsistent to mandate that the driver's licenses or state-issued ID cards include the date of birth, unless absolutely necessary. We recommend DHS consider alternative methods of identifying age of majority on driver's licenses and state-issued ID cards to avoid governmental disclosure of another piece of personal identifying information. Such methods could include indicating the month and year of the age of majority for driver's licenses or state-issued ID cards when the issuance date is underage or requiring re-issuance of cards when the age of majority is reached, thereby allowing cards issued to minors to be clearly identified without the need to include the precise birth date.

### **Background Checks**

The proposal requires states to conduct name-based and fingerprint-based criminal history records checks against state criminal records and the FBI's NCIC and IAFIS on employees working in state DMVs who have the ability to affect the identity information that appears on the driver's license or identification card, who have access to the production process, or who are involved in the manufacture of the driver's licenses and identification cards. The proposal also requires states to pay a fee to the FBI to cover the cost of this check and to conduct a financial history check on these employees. While our members encourage the use of background checks for DMV employees involved in sensitive positions, the proposal contains no guidance for states on what criminal history would bar prospective employees from said positions and even more troubling is the question of what information contained in their financial history would be used in employment decisions. In the absence of defined guidance for states, the implementation of this requirement could vary widely between states and could create a discriminatory climate based on the perceptions and biases of individual state legislators. We strongly

believe that a fair, equitable and consistent set of background requirements is essential for this process to be effective nationally.

If you have any further questions or comments on this matter, please do not hesitate to contact either of us or John Carlson, Executive Director of BITS at 202.289.4322.

Thank you for your consideration.

Sincerely,

Leigh Williams  
President  
BITS

Richard M. Whiting  
Executive Director and General Counsel  
The Financial Services Roundtable