June 4, 2007

To: Members, California State Assembly

From:

California Retailers Association
California Bankers Association
Association of California Insurance Companies
Association of California Life and Health Insurance Companies
American Electronics Association
American Resort Development Association
California Business Properties Association
California Financial Services Association
California Grocers Association
California Mortgage Bankers Association
California Restaurant Association
CTIA – The Wireless Association
California Independent Grocers Association
Direct Marketing Association
Information Technology Association of America
Personal Insurance Federation of California
Acxiom
AOL
Experian
Internet Alliance
NetChoice
Reed Elsevier
TechNet
Yahoo!
Comcast

RE: <u>OPPOSITION TO Assembly Bill 779 (Jones)</u>

The above businesses and associations strongly oppose AB 779 (Jones), which establishes onerous data management standards for business and government while exempting the bill's sponsors from those same requirements. In addition, the bill requires businesses and government to pay for the costs associated with reissuing "compromised" debit and credit cards – even in cases where the card numbers have NOT been compromised. Finally. AB 779 makes unnecessary changes to California's historic data-breach law, driving up costs of compliance for both businesses and government agencies.

The data security standards in AB 779 are <u>NOT</u> the industry data security standards. According to the author's office, Section One of the bill merely places into statute industry requirements for the protection of credit and debit card information called the Payment Card Industry (PCI) Data Security Standards. At a recent press conference on the bill, supporters argued that the bill simply requires business and government to do what they should already be doing, although the sponsors of the bill – the credit unions – have exempted themselves from the requirement. (This provision has never been heard in a committee in the Assembly. The language was amended in after the bill was heard in Assembly Judiciary and Assembly Business and Professions Committees and the author waived presentation of the bill in Assembly Appropriations).

We believe that an entity could be in compliance with the PCI standards, yet be in violation of state law if this bill passed. For example, under Requirement 3.2.1 of the PCI standards (Version 1.1, released September 2006), there are a few sentences of explanation for that requirement, including this one: "To minimize risk, store only those data elements needed for business." It is

simple explanation of ways minimize risks. But that sentence has been rewritten in AB 779. The bill lists under the list of PROHIBITED acts: "(3) [s]tore any payment related data that is not needed for business." Thus a guideline on how to minimize risks becomes a violation of state law. Worse, the term "not needed for business" is not defined anywhere in the bill. Businesses and government agencies trying to comply with the law would not have a predictable standard to live by. As a practical matter, the term will be defined in a court of law when the business is sued. Thus under PCI, a business can determine what constitutes "needed for business;" under AB 779 a judge will determine it after the fact.

There are other conflicts between the PCI language and the bill, but it will be impossible to conform the statute to the PCI standards because the standards change very frequently. The original PCI standards were in effect for about two years. The most recent version, published last September, has been in effect only since January of this year. The sponsor counters that the concepts remain the same. The problem is that as the language changes, businesses and government agencies will constantly face the problem of being in compliance with PCI but in violation of this bill if it becomes state law.

AB 779 forces businesses and government agencies to reimburse credit card issuers for replacing "compromised" credit and debit cards even when the cards have NOT been compromised. The credit unions say that large credit card breaches such as the one at TJX are costing them millions of dollars because they are forced to reissue compromised credit cards that have been "compromised." They say this bill is needed for them to recoup those costs. But they can do that already. In fact, the Massachusetts Credit Union League have already filed suit to recover those costs from TJ Maxx.

The sponsors say that their intent is to make retailers (or any entity that takes credit cards) pay when they are responsible for credit card fraud. But that is not what the bill does. AB 779 requires businesses and government agencies to pay for the reissue of credit cards when those businesses or government agencies finds that credit card or debit card numbers were "reasonably believed to have been, acquired by an unauthorized person." The banks or credit unions that issue the credit cards do not have to demonstrate that the credit or debit cards have actually been compromised.

Consider a common computer breach problem. A small business or government agency stores back-up tapes that contain credit or debit card numbers (and assume that information is stored in a manner that complies with the data security section described above). Now assume those tapes can't be found. So to comply with California's historic data breach law, the small business/government agency has to notify the 10,000 names on the tape and inform them of the breach. Now suppose that a week later the tape is found locked in a closet. It is clear that the information has not been compromised. However, under AB 779, the small business/government agency would still be required to pay the credit card issuers $250,000 ($25 x 10,000) – to replace credit cards that are clearly not compromised.

This is not a problem unique to the use of computer tapes. The problem is that AB 779 uses the threshold for the data breach law. The breach law is written so that consumers will be notified if

there is a reasonable belief that their personal information has been acquired. That is a long way from proof that credit or debit cards have been compromised.

This Legislature would never contemplate sending a person to prison based on a "reasonable belief" that the person committed a crime. Likewise, businesses and government agencies should not have to be forced to pay millions to credit card issuers just because there is a "reasonable belief" that those credit or debit cards may have been compromised.

AB 779 makes unnecessary changes to California's historic data breach law that will drive up the cost of compliance especially for small businesses. California was the first state to require notification of breaches of personal data on computers. Since its passage in 2002, many states have enacted similar laws, many which are nearly identical to California's law.

A key element of the law is the simplicity of the notice requirement. Data breaches happen to government, big business and small businesses. Mandating the content of the notice to fit all situations is simply not possible. But AB 779 adds a number of mandates that will cause problems for both large and small businesses. For example, the bill mandates that businesses and state agencies who are victims of a hacking have to devote a phone line (toll free if the company has a toll free line) to answering questions about the breach. The fact is that the business or agency won't be able to say much more than what was on the notice. But consider the small business that has a computer stolen. That business must now not only notify their customers of the theft (to comply with the data breach law), they have to devote employee time to repeating information on the notice. For larger businesses, the new requirements mean that businesses will have to write a California-only breach notice, again adding unnecessary cost to the notification process.

For all of these reasons, we urge that you **VOTE NO** on **AB 779.**