

## Privacy and Information Management

OCTOBER 2004

### Contacts

Lisa J. Sotto  
200 Park Avenue  
43rd Floor  
New York, NY 10166-0136  
(212) 309-1223  
lsotto@hunton.com

Margaret P. Eisenhauer  
Bank of America Plaza  
600 Peachtree Street, NE  
Suite 4100  
Atlanta, GA 30308-2216  
(404) 888-4128  
peisenhauer@hunton.com

### Additional Lawyers

Christopher Kuner  
Jan Dhont  
Tania S. Perez  
Ashley B. Rowe  
Aaron P. Simpson  
Courtney S. Stolz

### Center for Information Policy Leadership

Martin E. Abrams\*  
Fred H. Cate

\*Mr. Abrams serves as Senior Policy Advisor to Hunton & Williams' Center for Information Policy Leadership. He is not a lawyer.

## New Security Standards for Businesses That Maintain Personal Information

California recently became the first state to impose a general security standard on businesses that maintain personal information. The new law becomes effective on January 1, 2005.

A.B. 1950 requires businesses that own or license personal information about California residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorized access, destruction, use, modification or disclosure. In addition, businesses that disclose personal information to nonaffiliated third parties must contractually require those entities to maintain reasonable security procedures. Given the geographic reach of many organizations, the new California law effectively imposes a national security standard on businesses that maintain personal information.

### Scope of A.B. 1950

The new law applies to all businesses (other than those described below) that own or license personal information about California residents. The phrase "owns or licenses" includes (but is not limited to) personal information that a business retains as part of its internal customer account or for use in transactions with the person to whom the information relates. While the law is chaptered in the "customer records" title of the California Civil Code, based on the language of the law itself, A.B. 1950

appears to apply to both customer and employee information.

"Personal information" means unencrypted data consisting of a person's name, in combination with:

- a Social Security number,
- a driver's license or California ID card number,
- an account, credit card or debit card number along with a password or access code, or
- medical information.

The new law excludes from coverage entities that are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the California medical, financial and motor vehicle records privacy laws. In addition, any business that complies with another state or federal law providing greater protection to personal information is deemed to be in compliance with A.B. 1950.

### "Reasonable" Security Procedures Required

A.B. 1950 requires covered businesses to implement and maintain "reasonable" security procedures and practices, appropriate to the nature of the personal information, to protect the information from unauthorized access, destruction, use, modification or disclosure. The law does



not define what is “reasonable,” nor does it offer guidance on how to meet the reasonableness standard. This means covered businesses will need to define internally the security measures they consider both reasonable and appropriate in light of the scope of their operations and the nature and sensitivity of the personal information they maintain. While we anticipate that California courts will, over time, establish such standards, we recommend for now that companies rely on Gramm-Leach-Bliley Act (GLB) Safeguards Rule guidance when developing security programs.

## Contractual Requirements for Disclosure to Third Parties

The new law also requires businesses that disclose personal information about California residents to nonaffiliated third parties to contractually bind the third parties to implement and maintain reasonable and appropriate security procedures to protect the information. Thus, companies will now need to keep track of certain recipients of personal information (such as service providers), and require them by contract to implement appropriate security measures. Similar contractual requirements are found in GLB and HIPAA.

## Enforcement

California law permits individuals to sue for unlawful or unfair business practices. The new law does not require that an individual be harmed for a violation to occur. Given that existing California law requires organizations to notify individuals promptly of a security breach involving unencrypted computerized personal information, we anticipate a high level of enforcement activity as a result of A.B. 1950.

## Significance of A.B. 1950

As the nation’s first state law imposing a security standard on personal information retained by businesses not otherwise obligated by law to safeguard the information, A.B. 1950 will have an immediate impact on how many businesses maintain information about their customers and employees. The scope of the law casts a wide net, essentially mandating a national information security standard — today, even most modestly-sized entities conduct business in California.

As indicated above, A.B. 1950 builds on the controversial security breach notification law (S.B. 1386) passed in California two years ago. Under S.B. 1386, now chaptered at Cal. Civ. Code § 1798.82, businesses must disclose any breach in the security of their computer system to California residents whose unencrypted personal

information was acquired by an unauthorized person. When S.B. 1386 was enacted, critics charged that S.B. 1386 punished businesses that suffered security breaches even though their security procedures complied with legal requirements. The passage of A.B. 1950 fills that gap by imposing a new security standard designed to prevent the security breaches that require notification under S.B. 1386.

## We Can Help

By January 1, 2005, all businesses covered by A.B. 1950 must develop and implement reasonable security procedures to protect personal information from unauthorized access, destruction, use, modification and disclosure. Businesses that disclose personal information to nonaffiliated third parties also must have in place contracts requiring those entities to implement reasonable security procedures. Hunton & Williams’ Privacy and Information Management specialists assist clients in complying with evolving state and federal privacy requirements. We have experience assessing privacy risks, drafting policies and procedures to comply with legal requirements, and preparing contracts providing for the protection of personal information. If you have any questions about the significance of A.B. 1950, or would like assistance complying with the new law, please contact us.

© 2004 Hunton & Williams LLP. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.