



California, Texas Amend Data Breach Notification Laws; Texas Expands Health Privacy Requirements

California Amends Data Breach Notification Law: Mandates Attorney General Notification, Content Requirements

California has expanded its already stringent data breach notification law by adding significant new provisions, including a requirement to provide notice to the California Attorney General when the data breach involves more than 500 Californians. After former California Governor Schwarzenegger vetoed State Senator Simitian's data breach legislation in 2008, 2009 and 2010, the bill was finally enacted when current Governor Jerry Brown signed SB 24 on September 1, 2011. The existing California breach notification law requires businesses to give notice to California residents of breaches in the security of certain personal data. Although many similar laws require notice only when a risk of harm exists, California does not limit notification requirements to breaches involving a reasonable risk of harm, and the law is considered to be one of the broadest and most stringent in the nation. The new law comes into effect on January 1, 2012.

The newly amended Civil Code § 1798 now requires that data controllers notify the California Attorney General where a breach affects more than 500 California residents. The law also requires notice to the California Office of Privacy Protection when a commercial entity does not provide individual notice and instead relies upon "substitute notice," through websites and major statewide media if a breach affects more than 500,000 residents or where mail notice would cost more than \$250,000. In a move toward more prescriptive requirements, the law requires greater details in the content of notification letters. Required content now includes the types of information breached, the date or estimated date range of the breach, whether notification was delayed as a result of a law enforcement investigation, and contact information for credit reporting agencies. The law provides an exception for HIPAA-covered and compliant entities.

The new amendments may add a further burden to the California Office of Privacy Protection, which is facing increased pressures due to significant budget cuts. Under new budget cutting measures approved by Governor Brown on June 30, funding for the California Office of Privacy Protection was cut in half. The Governor's initial proposal, however, had proposed to eliminate the Office entirely.

Texas Amends Breach Notice Law to Have Extraterritorial Effect and Significantly Expands Health Care Privacy Requirements

Texas Governor Perry recently signed a new law that significantly expands both breach notification requirements and state health privacy requirements. Prior to the amendment and subject to certain exceptions, entities that conduct business in Texas and own or license computerized data that includes sensitive personal information were required to disclose any breach of system security to any resident of the state whose sensitive personal information was, or was reasonably believed to have been, acquired by an unauthorized person. Under the new law, such entities experiencing a breach will be required to provide notification to both affected residents as well as non-residents if the non-resident lives in a state that does not require notification to the individual of a breach of system security. For individuals residing in states outside of Texas that have breach notification laws, entities would be deemed compliant with the new law if they provided notification pursuant to such other laws. States that have not passed data breach legislation include Alabama, Kentucky, New Mexico and South Dakota. As a result of passage of this law, an entity doing business in Texas that experiences a breach within the meaning of the Texas statute could be required to provide notification of the breach to affected residents in all 50 states. The law also increased penalties for violations to \$100 per affected individual per day of failed or delayed notification, up to \$250,000 for a single breach. The law becomes effective September 1, 2012.

The new law also adds significant obligations to an existing Texas law that protects the privacy of health information. The new provisions, as well as existing provisions, apply to “covered entities,” a term broadly defined to include any entity that assembles, collects, analyzes, uses, evaluates, stores, transmits or comes into possession of protected health information. As such, the law reaches a much larger universe of entities than the federal privacy standards promulgated under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which apply to health plans, health care clearinghouses and health care providers that engage in certain electronic financial or administrative transactions as well as vendors of such entities that need access to protected health information to perform functions on behalf of such entities or provide services to them. Notably, the law would require individual authorization for the electronic disclosure of protected health information except for disclosures to other covered entities for treatment, payment, health care operations, or for the performance of insurance functions. It would also allow electronic disclosures in the absence of individual authorization as otherwise authorized or required by state or federal law.

The new Texas law could impose substantial costs on entities that have never before had to implement extensive protections for health information—including biannual employee training and training for new employees within 60 days of hire. Violations of these provisions are punishable by civil penalties of up to \$250,000 per violation, but may be subject to an annual cap of the same amount where disclosure is to another covered entity and certain other conditions are met. Multiple violations that constitute a pattern or practice are subject to a civil penalty of up to \$1.5 million.

Federal Data Breach Notification Law Under Active Consideration

The possibility of a new federal data breach notification law continues to be a hot topic on Capitol Hill, where multiple bills are being considered in both the House and Senate to create a federal standard for data breach notification. One of the primary impetuses for these bills is the increasingly complex and diverse state data breach notification laws which can impose a high compliance burden on interstate commerce. Although movement on these bills has slowed over the late summer months in light of debt and budget issues, significant privacy legislation, along with a data breach notification standard, may still pass in this Congress due to considerable bipartisan and business support. Contentious points remain, however, with respect to preemption, the scope of the definition of personal information, whether the federal standard will include a risk of harm trigger, and whether and to what extent agencies, and the FTC in particular, will have the power to issue regulations regarding the breach notification process.

If you have any questions regarding this update, please contact the Sidley lawyer with whom you usually work.

The Privacy, Data Security & Information Law Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers. Sidley provides services in the following areas:

- Privacy and Internet Litigation and Regulatory Advice
- Data Breach, Incident Response, and Cybercrime Advice
- Global Data Protection and Information Security
- International Data Transfer Solutions
- Outsourcing and Cross-Border Issues
- Gramm-Leach-Bliley and Financial Privacy
- HIPAA and Healthcare Privacy
- Workplace Privacy and Employee Monitoring
- Cyberlaw, E-Commerce, and Internet Issues
- Unfair Competition and Consumer Protection
- Trademark and Copyright Litigation and Counseling
- Website Policies and Domain Name Protection
- Records Retention and Electronic Discovery

To receive future copies of this and other Sidley updates via email, please sign up at www.sidley.com/subscribe

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

www.sidley.com

Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm's offices other than Chicago, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley or the firm.

SIDLEY AUSTIN LLP
SIDLEY