California Attorney General Issues 2012 Data Breach Report – Announces Investigating Breaches of Unencrypted Personal Information In Transit Will Be Enforcement Priority

In 2012, for the first time, companies and government agencies subject to California's Breach Notification Law were required to submit copies of their data breach notices to the California Attorney General when the breach involved the personal information of more than 500 California residents. The Attorney General recently released a report on her office's review of the 131 breach notices submitted by 103 different entities in 2012. Her report focuses on the role information security policies can play in protecting personal information, and urges companies to review their policies, tighten their security controls and encrypt personal information when "in transit", i.e., when moving or sending it out of their networks on portable devices or media or in emails. The Attorney General also recommended that the California legislature enact laws requiring the encryption of such "in-transit" personal information on portable devices and media and in email, and expanding California's breach notification law to require notifications of breaches of online credentials, like user names and passwords, that do not meet the current definition of "personal information" under the breach notification of law. Finally, the Attorney General announced that her office will make it an enforcement priority to investigate data breaches involving "in-transit" unencrypted personal information.

The Attorney General's report reviewed notices that were submitted for breaches of personal information for over 2.5 million Californians. The average (mean) breach size was 22,500 individuals; the median breach size was 2,500 individuals. Forty-nine percent of breaches were in the retail, finance, or insurance industries. The most frequently involved types of information were social security numbers, payment card information, and medical or health information.

The report found that 45 percent of the breaches "were largely the result of failures to adopt or carry out appropriate security measures," and in particular, "a failure to encrypt sensitive data when it is in transit on portable devices or in emails." To address these breaches, the Attorney General recommended that companies encrypt digital personal information on mobile media or when otherwise sending it out of their own networks and prioritize data security in employee training. The report noted that many of the breaches resulting from procedural failures "were likely the result of ignorance or noncompliance with organizational policies," underscoring to the Attorney General the importance of regular training in addition to strong controls.

The report further notes that, "[d]espite the incentive created by the breach notification law's exemption for encrypted data, many companies are still failing to use this effective security measure," and recommends the Legislature enact a law requiring use of encryption to protect personal information on portable devices and media and in email. The Attorney General also pledged to prioritize enforcement investigations of breaches involving such "in-transit" unencrypted personal information, and urged other government agencies to do the same.

The report also found that while California law requires that breach notices be written in plain language, the average reading level in the notices was 14th grade. The Attorney General recommends that companies engage communications professionals to help make notices more accessible.

Finally, the Attorney General indicated support for broadening the statutory definition of personal information within California's breach statute to include online credentials, like usernames or email addresses, in combination with passwords or security question and answer. Timely notice of breaches involving such data would, the report says, allow individuals the opportunity to protect themselves by changing their credentials. A bill to expand the definition passed the California State Senate on May 16th and appears poised to pass the Assembly following its summer recess.

California's Breach Notification Law was passed in 2003 and has become a model for forty-six other states. It presently requires that Californians be notified "in the most expedient time possible and without unreasonable delay," when there has been a breach of the security of computerized data if personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Breach notification laws often require complex and individuated analysis to determine what steps need to be taken to comply with an individual state's notification law. For more information regarding strategies for preventing or responding to data breach incidents or addressing other data privacy and security concerns you may have, please contact a member of our leading Privacy & Data Security team, including **Jim DeGraw**, **David McIntosh**, **Doug Meal**, and **Mark Szpak**.