California AG Cracks Down on Timing of Data Breach Disclosures

February 5, 2014 Ronald Breaux, Tim Newman

PRACTICES Healthcare Transactions and Regulatory, Healthcare and Life Sciences

Kaiser Foundation Health Plan, Inc. ("Kaiser") has agreed to pay $150,000 to settle claims by the California Attorney General (the "AG") that Kaiser's notification to California residents regarding a breach of their personal information was unreasonably delayed. In its suit, the AG alleged that Kaiser should have provided notice as soon as it determined that particular individuals' information had been or was "reasonably believed to have been" breached – even before Kaiser concluded its internal investigation. The case, *California v. Kaiser Foundation Health Plan, Inc*., is one of the first of its kind and will likely impact companies' data breach disclosure practices.

In the United States, disclosure of breaches of personal information (also referred to as "personally identifiable information" or "PII") is largely governed by the law of the state(s) where the affected individuals reside. Currently, 46 states, the District of Columbia, and several territories have enacted laws requiring companies to notify their residents of breaches involving personal information. Although the precise definition of "personal information" varies by state, it typically includes names combined with social security numbers, driver's license numbers, state ID card numbers, or financial information. Section 1798.82 of the California Civil Code ("the Notification Law") requires owners of computerized data to notify California residents of any breach that exposes their personal information ***"in the most expedient time possible and without unreasonable delay***, consistent with the legitimate needs of law enforcement . . . ***or any measures necessary to determine the scope of the breach*** and restore the reasonable integrity of the data system." Under California unfair competition law, any "unlawful, unfair or fraudulent business act or practice" – including breach of the Notification Law – constitutes "unfair competition" and the AG may seek injunctive relief and/or civil penalties.

In its complaint, the AG alleged that Kaiser learned in September 2011 that an external hard drive containing the personal information of its employees had been sold at a thrift shop to a person unaffiliated with Kaiser. By December 2011, Kaiser secured custody of the hard drive and began a forensic examination of the drive. The initial analysis, which was completed in December, allegedly revealed that the drive contained social security numbers and related personal information of at least 30,000 employees and some of their family members; but the forensic exam continued through at least February 2012. Kaiser notified the affected California residents in mid-March – about six months after it first learned of the breach and four months after it began its forensic analysis. According to the AG, this constituted "unreasonable delay." Interestingly, although the forensic examination of the drive continued through February 2012, the AG alleged that Kaiser had sufficient information to notify at least some of the impacted individuals in December 2011 and violated the Notification Law by failing to do so.

Kaiser has agreed to settle the AG's claims without admitting liability. In a stipulated judgment filed for the court's approval, Kaiser agreed to pay $30,000 in civil penalties and $120,000 in attorney's fees and costs of investigation and prosecution. Kaiser also agreed to an injunction against further violations of the Notification Law with respect to personal information of current or former employees. The injunction specifically requires Kaiser to provide notification of any future breaches

of employee personal information on a "rolling basis" where "feasible and appropriate," meaning Kaiser must provide notice "as soon as reasonably possible after identifying a portion of the total individuals affected by a breach, ***even if Kaiser's investigation of the breach is ongoing***" and must "continue to notify individuals as soon as they are identified, ***throughout and until completion of Kaiser's investigation of the breach."*** Within 120 days of the judgment, Kaiser must also undertake additional employment training; review its policies regarding encryption of emails containing employee personal information and devise a plan for updating those policies as needed; conduct an audit regarding employee access to employee personal information; and provide a report to the AG's office regarding its audit.

The AG's suit against Kaiser and the resulting settlement may have far-reaching implications for companies responding to a data breach. Relying upon the apparent flexibility of the phrase "without unreasonable delay" and the allowance for delayed notice when "necessary to determine the scope of the breach" – both of which are typically included in state disclosure laws – companies have often delayed notifications until they conclude their investigations. This has numerous advantages, including allowing the company time to determine what specific information was breached, reducing the number of "false positives" (notifications to unaffected individuals), minimizing the number of inadvertently inaccurate communications regarding the breach, and allowing the company a measure of control over the public relations aspect of disclosure. Given the AG's lawsuit and the resulting settlement, however, this measured approach may no longer be an option – at least where California residents' information may have been involved in a breach. The case may also inspire other attorneys general to narrowly interpret their own states' "unreasonable delay" clauses.

Given the rapidly evolving state of cybersecurity law and the massive liability that breached companies can face, we strongly recommend that companies engage legal counsel immediately upon receiving notice that a breach may have occurred. Haynes Boone provides investigation, remediation, and disclosure services to companies that suspect a breach and represents them in resulting regulatory actions, litigation, and other disputes. For additional information, please contact one of the attorneys listed below.

Ronald W. Breaux
214.651.5688

David Siegal
212.659.4995

Emily Westridge Black
214.651.5221

Timothy Newman
214.651.5029
