Company Settles with State Attorney General Over Failure to Disclose Data Breach

By Tim Newman | July 11, 2011

WellPoint, Inc. recently reached a settlement with the Indiana Attorney General following its failure to disclose a security breach involving consumers? personal information. WellPoint is the latest in a string of companies that have run afoul of the evolving disclosure rules which may be triggered when a company?s data is hacked or otherwise accessed without authorization. In the United States, nearly all of the states have adopted disclosure rules in the past several years, and a failure to comply with the rules can result in substantial liability and loss of goodwill. Companies that collect, maintain, or transmit personal information should learn from the lessons of others and consider taking the following steps: (1) develop sophisticated defenses to avoid a breach and document the steps taken, (2) if a breach is suspected or reported, fully and promptly investigate it, and (3) if a breach has in fact occurred, timely disclose the breach in accordance with the law.

Haynes Boone has experience advising public and private companies regarding compliance protocols in advance of any breach as well as appropriate responses after a breach has occurred. For more information, please contact any of the attorneys at the bottom of this alert.

WellPoint Allegedly Failed to Secure Personal Information or Disclose a Breach

WellPoint, a health insurance provider located in Indianapolis, Indiana, hosted an online health insurance application for its customers. In order to submit applications online, customers were required to provide their name, date of birth, Social Security number, and certain financial account information. When customers completed their applications, they received a hyperlink to WellPoint?s website that allowed them to track the status of their applications.

The Indiana Attorney General?s Office alleged that WellPoint made several missteps. First, WellPoint failed to adequately protect consumers' personal information as the information was submitted. The Indiana Attorney General alleged that unauthorized individuals could easily manipulate the hyperlink?s Uniform Resource Locator (or ?URL?) to view more than 32,000 applicants? unencrypted personal information.

Second, WellPoint failed to adequately investigate reports of a potential breach. According to the Attorney General?s Office, in February 2010 a consumer notified WellPoint that its data may have been breached through URL manipulation. WellPoint made an unsuccessful attempt to call the complaining consumer, but took no other action to investigate the alleged breach or to secure consumers? data. Indeed, WellPoint did not actually secure the personal information at issue until after it was served with a class action complaint related to the breach in March 2010.

Finally, WellPoint failed to timely report the data breach in compliance with applicable laws. Indiana?s Disclosure of Security Breach Act is typical of many states? data breach disclosure laws. Under the Indiana law, any company that owns computerized data that includes the personal information of Indiana residents must disclose a data breach to affected individuals and the Indiana Attorney General if (1) the information is unencrypted or the information is encrypted and was or may have been acquired by someone with access to the encryption key, and (2) the company ?knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception . . . identify theft, or fraud . . . .? ?Personal information? consists of either

an individual?s Social Security number or an individual?s first name (or initial) and last name accompanied by (1) a driver?s license or state identification card number, (2) a credit card number or (3) a financial account number in combination with a security code, password, or access code that would permit access to the person?s account. Importantly, the disclosure of the breach must be made ?without unreasonable delay.? A company may only postpone disclosure if a delay is necessary to secure the integrity of the computer system or identify the scope of the breach, or if a delay is requested by the Indiana Attorney General or other law enforcement agency.

The Indiana Attorney General further alleged that in June 2010, nearly four months after WellPoint received notice of the potential breach, WellPoint began disclosing to Indiana consumers that their personal information may have been accessible to unauthorized individuals through WellPoint?s website. The Indiana Attorney General?s Office stated that it never received a disclosure from WellPoint.

Indiana Attorney General?s Action and Settlement

The Indiana Attorney General sued WellPoint in October 2010 for its failure to disclose the breach to consumers ?without unreasonable delay? and its failure to disclose the breach to the Attorney General. The Attorney General further alleged that no law enforcement agency had requested a delay of the required disclosure.

WellPoint recently settled these claims, admitting that Indiana residents? personal information had been accessible for more than four months before the company took action to secure it and that it failed to disclose the breach to the Attorney General when it finally notified consumers. WellPoint agreed to (1) provide two years of credit monitoring and identify theft protection to Indiana residents whose data was accessible through WellPoint?s online application tool, (2) reimburse proven identify theft losses resulting from the breach (up to $50,000 per individual), (3) abide by Indiana?s data breach disclosure laws, and (4) pay $100,000 to the Attorney General for fees and costs in this case and to support the state?s future consumer protection efforts.

The Lessons for Other Companies Handling Consumers? Personal Information

The WellPoint settlement highlights several best practices that affected companies should consider adopting. First, companies should consider taking steps to ensure the security of consumers? personal information. It is important for companies collecting and storing personal information of individuals to protect this personal information at every stage by, for example, adopting encryption protocols. Second, companies should consider establishing procedures for promptly investigating and responding to any suspected or reported breach. Many companies choose to adopt policies that identify specific employees responsible for investigating any breach and documenting the steps taken. Finally, if a breach is discovered, companies should consult with counsel to evaluate the applicable disclosure laws and take steps to comply with those laws. Disclosure requirements vary by state, and requirements are usually triggered by the citizenship of the individuals whose data is disclosed. The company?s principal place of business or geographic location is typically immaterial. Thus, the scope of required disclosure is potentially very broad, and must be made on a state-by-state basis. By taking these measures, companies may avoid costly litigation and fines resulting from a failure to appropriately respond to a breach of the security of individuals? personal information.

For additional information, please contact one of the attorneys listed below. ***You may also view the alert in the PDF attached below.***

Ronald W. Breaux
214.651.5688

David Siegal
212.659.4995

Emily Westridge
214.651.5221

Timothy Newman
214.651.5029

PDF - Data_Breach.pdf