Anthem Cybersecurity Attack Highlights Threat to Health Care Data Security

February 16, 2015

On February 4, 2015, Anthem Blue Cross Blue Shield announced that it had experienced a cyberattack which exposed sensitive data of up to 80 million customers. The attack is the largest healthcare breach to date, and compromised customer records from all 50 states.

Since the breach, class action lawsuits have been filed in Alabama, California, Georgia, and Indiana. All four complaints allege that Anthem failed to take adequate steps to safeguard its customers' sensitive data. The suits also allege that timely notice of the data breach was not provided to customers because Anthem waited eight days before going public with information about the cyberattack. The class actions all claim that customers would not have purchased Anthem's health insurance products if they had known the company failed to provide adequate security safeguards. The Alabama suit also alleges the "immediate and imminent danger of identity theft" stemming from the data breach. It is alleged that, to date, Anthem's promise to provide customers with free credit monitoring and identity theft protection has yet to be implemented, leaving customers vulnerable to malicious use of the stolen sensitive data.

Similar attacks on the health care industry should be anticipated in the future. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 require health insurers to follow strict privacy and security regulations, and to pay substantial fines if they do not. Nonetheless, the health care industry does not always recognize that customer demographic information divorced from medical diagnosis or treatment—such as customer name, address, birth date and Social Security Number—is subject to the HIPAA/HITECH rules. The government HIPAA enforcement agency, however, does consider this kind of information to be subject to HIPAA/HITECH, and has levied fines against health care entities in the past for failing to adequately protect it.

It has been suggested that health care entities are slow to adopt state-of-the art-security practices or fail to adopt adequate security measures altogether, even though stolen medical information is sometimes even more valuable to hackers than credit card information. For example, the health care sector has been criticized for failing to store sensitive customer information in separate databases which can be walled off in case of an attack, or to encrypt such data at rest in the health insurer's computers. While HIPAA and HITECH do not mandate encryption of data at rest, many experts (including government enforcers) believe that it is a best practice that should be adopted absent some extremely compelling reason to use a different security protection for data at rest.

Historically, the government enforcers of HIPAA stated that the risk of stolen or lost laptops or smart phones posed a far more serious threat to protected health information than hacking. These enforcers recently reported to Congress that hacking only affected 115,900 individuals in 2011, and was only the fourth-largest threat to health care privacy. The Anthem breach, affecting the third-largest health insurer in the United States and about a quarter of the United States population, is a wake-up call to the health industry and to government enforcers that hacking is a much more serious threat than previously thought. Assuming that Anthem ends up in the crosshairs of a HIPAA/HITECH government enforcement investigation, it could be subject to very significant civil money penalties, in addition to any money damages that it may have to pay to the plaintiffs in the pending class action lawsuits. The lesson to the health care industry is clear–take cybersecurity extremely seriously for all customer data and implement the best security management practices reasonably available.

Dykema will continue to monitor the outcome of the Anthem cybersecurity attack as more information becomes available. For more information on this article or cybersecurity legal obligations generally, please contact **Jonathan Feld** at (312) 627-5680, **Joanne Lax** at (248) 203-0816, any of the attorneys in Dykema's cybersecurity practice group, or your relationship partner.

Attorneys

Sherrie L. Farrell

Jonathan S. Feld

Practice Areas

Health Care