HALL RENDER
KILLIAN HEATH & LYMAN

HEALTH LAW NEWS

AUGUST 28, 2017

CYBERSECURITY INSURANCE CARRIERS: ARE YOU READY?

A recent U.S. Court of Appeals decision increases chances for data breach victims to successfully sue. In 2014, customers of a health insurer filed a lawsuit after their personally identifiable information ("PII") was revealed in a data breach that affected more than one million individuals.[1] The lower court dismissed the lawsuit in 2014, but on August 1, 2017, the U.S. Court of Appeals for the District of Columbia reinstated the lawsuit after finding that the customers faced a substantial risk for identity theft and that the health insurer was fairly traceable in having created the risk by not properly storing customers' personal data or maintaining adequate safeguards to protect customers' sensitive records.

While this opinion raises new liability concerns for health insurers and health care providers who fail to protect their customers from data breaches, cybersecurity insurance carriers ("Carriers") should also take note. Class standing in data breach cases is gaining traction and will impact the ability of Carriers to offer relevant third-party policies at reasonable prices. Many health care entities have either purchased or are considering purchasing third-party cyber insurance policies to cover losses that an entity causes to its customers and others, such as harms arising from the exposure of PII through a data breach. However, health care entities have expressed confusion and frustration when buying and renewing cyber insurance, and some entities are reluctant to purchase cyber insurance because of the high premiums and lack of certainty in coverage.

To get ahead of the increase in costs that will arise when more breach victims achieve class standing in a lawsuit, Carriers should make certain they understand the standard established by this case and begin to assess their cyber risk management strategies and approaches used with their insureds to manage costs appropriately. Otherwise, the current wide ranges of risk estimates and pricing for cyber insurance premiums will keep entities from renewing or purchasing cyber insurance.

CUSTOMERS' INJURY NEED NOT BE "ACTUAL OR IMMINENT"

The court held that because the health insurer allowed their customers to fall victim to the data breach, the health insurer improperly exposed them to a substantial risk of future identity theft, and therefore the customers did not need to show that they suffered an actual or imminent injury. Rather, the customers plausibly met the "substantial risk" standard since the health insurer's alleged negligence involving the data breach was enough to demonstrate that the customers were subject to a "sufficient and particularized" injury. The court found that even if credit card and Social Security information had not been stolen, the customers had standing to bring suit because of the risk for "medical identify theft."[2]

THE COURT IMPOSES A "FAIRLY TRACEABLE" STANDARD

Additionally, the customers sufficiently showed that the data breach was fairly traceable to the health insurer. The court did not explore if a proximate cause argument could insulate the health insurer from the lawsuit. Instead, the court reasoned that the customers' substantial risk of injury was "fairly traceable" to the health insurer's alleged conduct, even though the health insurer was not accused of affirmatively causing the data breach.

While in the past, causation for breach-related class action suits has been difficult to establish, this case is setting a precedent of a very low threshold for consumers to establish standing in a data breach lawsuit. In accordance with this case decision, so long as the breach can be fairly traced back to the entity that suffered the breach and the victims can demonstrate a substantial risk of harm, breach victims can seek recourse when the entity was negligent in protecting their PII.

PRACTICAL TAKEAWAYS

Given that cyberattacks are becoming more sophisticated, malware is becoming smarter and the cybercrime market is growing, Carriers should expect a continued increase in data breaches and class action lawsuits and plan accordingly. Carriers should consider the following as they continue to develop ways to quantify risks associated with data breaches and provide meaningful, affordable cyber insurance.

- Create clear and concise policy coverage terms to eliminate coverage confusion for the insured.
- Develop minimum cyber risk management controls and procedures and offer increased coverage at fair and reasonable rates based on

the insured's level of self-protection.

- Carefully review the insured's network security policies, crisis response plans and other security controls and provide cybersecurity best practices to the insured to help improve the insured's cyber risk posture.

If you have questions about this case or about how data breaches are impacting cybersecurity insurance, please contact Charise R. Frazier at cfrazier@hallrender.com or (317) 977-1406 or your regular Hall Render attorney.

Special thanks to Amanda Ray, law clerk, for her assistance with the preparation of this article.

[1] *Attias v. Carefirst, Inc.,* No. 12-7108, 2017 WL 3254941 (D.C. Cir. Aug. 1, 2017).

[2] *Id.* at *6.