Fourth Circuit Ruling Makes Data Management Policies More Important than Ever

By: Robert Van Arnam

07.13.2018

The Fourth Circuit has just made it easier for plaintiffs to bring data breach cases. The Court?s decision means more data breach cases will survive a challenge based on standing and makes creating and following data management policies more important than ever for entities that collect and store data.

On June 12, 2018 the U.S. Court of Appeals for the Fourth Circuit published its decision in *Hutton v. National Board of Examiners in Optometry, Inc.* The unanimous opinion clarifies what a plaintiff bringing a data breach case in the Fourth Circuit must show to prove standing. In what may prove to be a notable case for victims of data breaches, the court in *Hutton* held that the plaintiffs had standing to sue because they had been ?concretely injured by the data breach because the fraudsters used ? and attempted to use ? the Plaintiffs? personal information?? and because the complaints showed ?it is both plausible and likely that a breach of the database of the Board of Examiners in Optometry, Inc. (?NBEO?) resulted in the fraudulent use of Plaintiffs? personal information?.? Notably, the court pointed out that this *attempted* use qualified as an injury in fact even if the plaintiffs suffered no actual pecuniary harm.

The facts of *Hutton* are all too familiar. The plaintiffs provided NBEO with personal information as part of their application to sit for their respective national optometry examinations. The NBEO retained that data even after it had become outdated; at least two plaintiffs no longer used the last names under which they had applied to sit for their exams. At some point, the NBEO data was impermissibly accessed and shared. The plaintiffs received unsolicited credit cards in the mail; fraudulent Chase Amazon Visa accounts had been opened using stolen personally identifiable information. The plaintiffs determined that NBEO was the source of the data used to open the fraudulent accounts and, therefore, brought suit against NBEO.

The decision in *Hutton* is interesting because the facts are so common. An entity collected personally identifiable information, with permission, and for a legitimate purpose. The entity later allegedly

experienced a data breach, customer information was used, and plaintiffs sued the entity. Before *Hutton*, defendants could limit litigation costs and overall liability exposure by arguing that the plaintiff lacked standing to sue, often because the plaintiff did not experience financial harm. In this instance, however, the defendant?s motion to dismiss was denied because use of data, alone and without financial harm, provided the plaintiffs with standing to bring the case.

How, then, can entities help limit their exposure? A well thought out and enforced data management policy could have limited NBEO?s exposure. A data management policy, if followed, can limit the amount of data retained and require periodic breach testing of networks. An effective data management policy can also provide for regular forensic investigations of an entity?s systems to identify prior breaches. While this may sound like added cost to many managers, on balance it can easily pay for itself. In the long run, data management policies, privacy policies, and similar documentation, are much cheaper than litigation and are among the best ways that companies can limit their exposure to data breach lawsuits.

Related People

- Robert Van Arnam ? 919.981.4055 ? rvanarnam@williamsmullen.com

Related Services

- Data Protection & Cybersecurity
- Intellectual Property