Causation and Harm In Data Breach Litigation

Demonstrating that a data breach has resulted in an injury-in-fact can be difficult, because it is not always clear what has happened or will happen with the stolen data.

by Brian Ellman and Jee-Yeon Lehmann; Analysis Group, Inc.

Originally published in Cybersecurity Law & Strategy

Brian Ellman

Jee-Yeon Lehmann

Data breaches can have substantial adverse impacts on firms, not only in the form of negative publicity or harm to a company's brand and revenues, but through litigation that may result. A key point of contention in data breach litigation has been whether plaintiffs have met the injury-in-fact standing requirement of Article III of the Constitution. Demonstrating that a data breach has resulted in an injury-in-fact can be difficult, because it is not always clear what has happened or will happen with the stolen data.

For example, suppose hackers gained access to consumers' personal information but the information has not yet been misused. In that case, the breach will not have resulted in actual economic harm to the consumers even though risk for future harm from the breach may remain. As a result of this dynamic, plaintiffs in data breach litigation typically allege harm in terms of something that *could happen* (*i.e.,* an *increased risk* of future injury) rather than something that *did happen*.

The determination of standing under Article III also hinges on whether the present or future alleged harm was *caused* by the data breach in question, as opposed to another independent event or factor. Because of the conjectural nature of harm in many

data breach litigations, the inference of causation can be complex. For litigators on both sides of data breach cases, the framework for assessing causal relationships in product liability litigation for pharmaceuticals and medical devices may provide helpful guidance. In this framework, assessment of a causal relationship occurs through two levels of inquiry:

General Causation: Whether exposure to a product is plausibly related to the adverse outcome being alleged; and

Specific Causation: Whether a specific plaintiff's exposure can be shown to have been the cause of a particular adverse outcome as opposed to any other risk factor.

For a causal relationship to be established, the answer to both of these inquiries must be "yes." For example, in the multidistrict litigation involving the cholesterol drug Lipitor, plaintiffs alleged that Pfizer had failed to adequately warn users that exposure to certain doses of the drug was causally associated with a previously undisclosed increased risk of type 2 diabetes. In one ruling, a district court found that plaintiffs did not establish a general causal link between exposure to the drug at one of the specified dosages and the onset of diabetes. Additionally, the court found that plaintiffs failed to establish that the onset of diabetes was specifically caused by Lipitor exposure (at any dosage) as opposed to some other risk factor.

How can one apply a similar framework to data breach cases? Consider a breach in which hackers obtained contact information (*e.g.,* email addresses) of a number of website users. Suppose these website users then bring a suit alleging that they now face an increased risk of financial identity theft. Could the plaintiffs demonstrate a causal connection between the at-issue breach and alleged harm?

General Causation

The *general causation inquiry* might initially focus on the existence of a plausible and proximate causal link between the information obtained from the breach and the alleged injury. Despite the breach, an e-mail address, in itself, may not be sufficient to cause the harm alleged by plaintiffs — substantially more information is likely needed to open fraudulent accounts based on fake identities. In other words, because the particular data that were stolen in this hypothetical breach would not be plausibly and proximately related to financial identify theft, there would be no evidence of general causation. This would be similar to the finding in the Lipitor MDL that a specified dosage was below the level needed to establish a causal link to the onset of type 2 diabetes.

Suppose instead that a data breach resulted in the theft of a more comprehensive set of consumers' personally identifiable information (PII) (*e.g.,* contact information, social security numbers, banking information, passwords, and security questions and answers). In this case, plaintiffs may be able to establish that such a breach could plausibly lead to financial identity theft, thereby satisfying the general causation requirement.

Specific Causation

The inquiry would then move to the *specific causation* stage, which would focus on the question of the likelihood that this particular breach could be shown to be responsible for the alleged harm, independent of other causes. For example, if the stolen information were already accessible to potential misusers due to another data breach of many of the same people, the connection between the particular data breach at issue and the injury would be confounded. In such a situation, plaintiffs would likely be required to establish a more precise link between the at-issue breach and the alleged harm to survive the specific causation inquiry.

A recent case, *Hutton v. National Board of Examiners in Optometry (NBEO)*, No. 17-1506 (Fourth Cir. June 12, 2018), provides an example of a case in which plaintiffs were able to establish both general and specific causation. In *Hutton*, a group of optometrists noticed that credit card accounts had been fraudulently opened in their names. They determined that the only common entity to which all of them had provided the necessary personal information to open credit card accounts was the NBEO, an organization to which every optometry graduate had to submit personal information such as social security numbers as part of board certification exams. The optometrists sued NBEO, claiming, *inter alia*, negligence and breach of contract. A district court dismissed the suit for lack of Article III standing, but the Fourth Circuit Court of Appeals reinstated it. The appeals court held that plaintiffs had established, first, that the theft of information from the breach could cause the alleged injuries (general causation); and, second, that those injuries could plausibly be traced to the specific breach in question (specific causation).

Analysis

Clearing the threshold of establishing general and specific causation in a typical data breach litigation will often be difficult. Litigators applying the framework to data breach litigation would do well to familiarize themselves with the particular type and amount of data that were allegedly part of the breach. What information were available elsewhere? How plausible is the connection between those data and the claimed injury? Consideration of these and other elements will help litigators formulate approaches that can maximize their clients' chances of prevailing in the litigation.

Brian Ellman and Jee-Yeon Lehmann are vice presidents in the Washington, DC and Boston offices of Analysis Group, Inc., respectively.