Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Data Breach Dismissals Continue Post-Clapper

Law360, New York (July 18, 2014, 11:09 AM ET) --

David M. Brown Jr.

The U.S. Supreme Court's decision in Clapper v. Amnesty International USA continues to be relied on by federal courts to hold that "mere loss of data" or "increased risk of identity theft" in a data breach case does not constitute an injury that confers constitutional standing.

In re Science Applications International Corp. Backup Tape Data Theft Litigation involved the theft of a GPS system, stereo and several data tapes from a parked car. The tapes belonged to an employee of Science Applications International Corp., an information-technology company that handles data for the federal government. The stolen tapes contained personal and medical information for 4.7 million members of the U.S. military and their families who were enrolled in Tricare, which provides insurance coverage and health care to service members and their families.

The data breach victims asserted 18 causes of action against SAIC, alleging injuries for increased risk of identity theft, expenses for mitigating the risk of identity theft; loss of privacy, loss of value of their medical and personal information and SAIC's failure to meet the requisite standard for data security. SAIC moved to dismiss all of the claims on the ground that the plaintiffs lacked standing. The court agreed and dismissed almost all of the plaintiffs, noting that "the mere loss of data — without evidence that it has been either viewed or misused — does not constitute an injury sufficient to confer standing."

The court noted that the case "presents thorny standing issues regarding when, exactly, the loss or theft of something as abstract as data becomes a concrete injury." For example, the plaintiffs claimed that they are 9.5 times more likely than the average person to become victims of identity theft, and that their increased risk is enough to confer standing, which is a typical argument made by plaintiffs in data breach cases, although the probability factor differs. But invoking Clapper, the court held this is insufficient to confer standing, stating that the "degree by which the risk of harm has increased is irrelevant — instead, the question is whether the harm is certainly impending."

In Clapper, the plaintiffs, who were individuals and organizations that worked with foreign clients, contended that they were likely to be targeted for surveillance under the Foreign Intelligence

Surveillance Act. The Supreme Court ruled that the plaintiffs did not have an "injury in fact" (i.e., they lacked standing) because the threat of surveillance was too speculative. The court noted that the chain of events that still needed to occur before the plaintiffs would actually be harmed was not "certainly impending." The court reasoned that the plaintiffs would be harmed by FISA only if: (1) the government decided to target communications involving their clients under FISA, (2) the Foreign Intelligence Surveillance Court authorized the eavesdropping, (3) the government succeeded in obtaining their targets' phone calls or emails and (4) the plaintiffs were involved in the communication that the government actually intercepted. The court found that this "highly attenuated chain of possibilities does not satisfy the requirement that threatened injury must be certainly impending."

Similarly, in In re Science Applications International Corp., the court identified a lengthy chain of events that needed to occur before the plaintiffs' injury from identity theft became "certainly impending": "First, the thief would have to recognize the tapes for what they were, instead of merely a minor addition to the GPS and stereo haul. Data tapes, after all, are not something an average computer user often encounters. The reader, for example, may not even be aware that some companies still use tapes — as opposed to hard drives, servers or even CDs — to back up their data. Then, the criminal would have to find a tape reader and attach it to her computer. Next, she would need to acquire software to upload the data from the tapes onto a computer, otherwise tapes have to be slowly spooled through like cassettes for data to be read. After that, portions of the data that are encrypted would have to be deciphered. Once the data was fully unencrypted, the crook would need to acquire a familiarity with Tricare's database format, which might require another round of special software. Finally, the larcenist would have to either misuse a particular plaintiff's name and Social Security number or sell that plaintiff's data to a willing buyer who would then abuse it."

The court continued, "At this point, we do not know who she was, how much she knows about computers or what she has done with the tapes. The tapes could be uploaded onto her computer and fully deciphered, or they could be lying in a landfill somewhere in Texas."

The court also rejected the plaintiffs' argument that the cost incurred to prevent and mitigate the risk of identity theft creates standing. According to the court, the "plaintiffs cannot create standing by 'inflicting harm on themselves' to ward off an otherwise speculative injury."

The plaintiffs also argued that they had standing based on certain statutory violations (e.g., the Fair Credit Reporting Act) that automatically establish damages or a right to payment. The court rejected this argument as well, noting: "Standing, however, does not merely require a showing that the law has been violated, or that a statute will reward litigants in general upon showing of a violation. Rather, standing demands some form of injury — some showing that the legal violation harmed you in particular, and that you are therefore an appropriate advocate in federal court."

The court's decision that these plaintiffs lacked standing is consistent with many other courts' decisions in data breach cases post-Clapper. There are many hurdles facing plaintiffs in data breach cases, among which standing is paramount, and this case illustrates the speculative nature of many data breach injury claims when plaintiffs rush to sue before the dust settles.

—By David M. Brown Jr., Montgomery McCracken Walker & Rhoads LLP

David Brown Jr. is an associate in Montgomery McCracken Walker & Rhoads' Philadelphia office, where he is a member of the firm's litigation department.