wiley

NEWSLETTER

D.C. Circuit Data Breach Standing Decision Will Encourage More Litigation Over Security in New Technology

August 2017

On August 1, 2017, the U.S. Court of Appeals for the D.C. Circuit held that plaintiffs in a data-breach class action had sufficiently alleged Article III standing based solely on allegations that the theft of their personal information may be used in the future to cause them harm. *Attias v. CareFirst, Inc.*, 2017 WL 3254941 (D.C. Cir. 2017). This is the strongest indicator to date that class action data breach litigation is alive after the Supreme Court of the United States' decisions in *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016) and *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013).

While several circuit courts have dismissed data breach class actions on standing, *Attias* gives plaintiffs' lawyers incentive to continue to litigate, especially given the possibility of a favorable forum. In addition to confirming a need for guidance from the Supreme Court, *Attias* is a reminder that companies can expect the plaintiffs' bar to scrutinize and sue over data security in a variety of contexts.

Legal Standing in Breach Cases Is Unsettled

To establish injury in fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical." L*ujan v. Defenders of Wildlife*, 504 U.S. 555,560 (1992); *Spokeo*, 136 S.Ct. 1540 (2016). In the data breach context, harms associated with stolen personal information, like identity theft, often do not immediately follow the data breach, if they occur at all. As a result, courts are left to struggle with whether a potential future harm is enough for standing.

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

In assessing such prospective harms, the Supreme Court held in *Clapper* that "[a]llegations of possible future injury" do not satisfy constitutional standing requirements. 133 S.Ct. 1138, 1147. Rather, the "threatened injury must be certainly impending to constitute injury in fact." *Id.* That does not mean that plaintiffs are required to show that it is "literally certain that the harms they identify will come about." *Id.* at 1150 n. 5. But they must at least demonstrate a "substantial risk that the harm will occur." *Id.*

For years, plaintiffs have mostly—but not always—failed to convince courts that having personal information stolen constitutes an injury for Article III purposes. Most courts have held that the mere possibility that a hacker might use stolen information for identity theft or financial fraud at some point in the future was too speculative to constitute a case or controversy. *See*, e.g., *Whalen v. Michaels Stores, Inc.*, 2017 WL 1556116 (2nd Cir. 2017) (Plaintiff failed to allege standing post data breach "because [she] neither alleged that she incurred any actual charges on her credit card, nor, with any specificity, that she had spent time or money monitoring her credit.") However, not all courts have come out this way: the Seventh Circuit has held that loss of personal information can create standing. *See Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015).

There have been two recent Supreme Court decisions on this issue. In *Clapper*, the Supreme Court rejected standing of plaintiffs who sued to have a part of U.S. surveillance law struck down, claiming they feared incidental collection of their communications and were harmed by taking measures to avoid collection. The Court in *Clapper* found, "'[a]llegations of possible future injury' are not sufficient," making an "objectively reasonable likelihood" of future harm inadequate to proceed. *Clapper*, 133 S. Ct. at 1147. Last year, the Court held in *Spokeo* that, "[a]lthough tangible injuries are perhaps easier to recognize, we have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete." *Spokeo*,136 S.Ct. at 1549. Determining when a harm is both intangible and concrete often is not easy.

The *Attias* Case Presents Now-Familiar Facts

Attias presents fairly common data breach allegations. In 2014, hackers allegedly gained access to CareFirst's servers which contained personal identifiable information and personal health information of CareFirst's customers. The hackers were able to steal the customer data, which was not encrypted. Customers then sued in a purported class action, alleging that CareFirst failed to take reasonable steps to protect their data.

As in many data breach class actions, the district court held that the plaintiffs' alleged injury was too speculative to confer standing. *See Attias v. CareFirst, Inc.*, 199 F.Supp.3d 193 (D.D.C. 2016) ("merely having one's personal information stolen in a data breach is insufficient to establish standing to sue the entity from whom the information was taken."). The district court reasoned that plaintiffs had not experienced financial loss, and the chain of events describing any future loss—which involved unknown hackers at an unknown point in the future electing to use the stolen personal information for monetary gain—was too attenuated.

The D.C. Circuit Adds to Uncertainty, Confirms Data Breach Litigation May Be Worthwhile for Plaintiffs

The D.C. Circuit reversed the district court's *Attias* decision, siding with the Seventh Circuit on the issue of standing in data breach cases and furthering a circuit split on what constitutes an injury after a data breach. Compare *Whalen*, 2017 WL 1556116 (2nd Cir. 2017 (plaintiff did not suffer injury in fact) with *Remijas*, 794 F.3d at 693 (7th Cir. 2015) (plaintiff did suffer injury in fact). As the D.C. Circuit explained, "an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative—at the very least, it is plausible—to infer that this party has both the intent and the ability to use that data for ill." *Attias*, 2017 WL 3254941, at *6.

The D.C. Circuit held that the plaintiffs had standing based on allegations that the theft of credit card and social security information created a risk of identity theft. The complaint further alleged that the theft of customers' names, dates of birth, email addresses, and subscriber identification numbers, when combined, created a substantial risk of "medical identity theft," which involves obtaining medical services in the victim's name. The court found that the risk of this type of injury—even without the loss of social security numbers and credit card information—was sufficient.

More Litigation Will Follow, Impacting Emerging Technologies Like the Internet of Things, Big Data, and Artificial Intelligence

Standing in the data breach context is ripe for additional Supreme Court guidance. *Spokeo* has not produced uniform results, and a post-*Spokeo* Circuit split of authority has emerged. Innovations in standing doctrine can impact other areas as well. As we look to an increasingly connected future, and confront malicious action by criminals and nation states, what can we expect after *Attias*?

Data breaches will continue. As Verizon Enterprise Solutions predicts, "The triple threat of hacking, malware, and social has been on top and trending upward for the last few years, and it does not appear to be going away any time soon." Verizon Data Breach Investigations Report (2017). Other security issues will continue to emerge, as networks and devices are compromised for various nefarious reasons.

Legal divisions over standing allow forum shopping by plaintiffs in national data breaches. The threat of litigation and exposure are tremendous. *See* "Anthem Agrees to $115 Million Settlement of Data Breach Lawsuit" *The Wall Street Journal* (June 23, 2017), available here. The sheer size of such exposure may force companies to settle meritless claims to avoid vexatious litigation. This may result in large payouts to attorneys with little improvement in security.

To the extent these issues are litigated, we may see courts deciding what constitutes reasonable data security policy, such as whether the alleged lack of encryption in *Attias* was reasonable. Courts may also have to speculate about the motives or future actions of unknown hackers. This will be a particularly difficult area for courts to make law. Perhaps worse, we may see issues resolved in settlement documents, as companies look to avoid crushing litigation costs and unpredictable liability. Federal agencies and other experts are looking at these issues and developing standards of care that may be more helpful than settlement agreements available on court dockets.

Fundamentally, a lesser standard for Article III standing in cybersecurity-related cases (like the approach taken by the D.C. Circuit and the Seventh Circuit) will make it easier to bring security-related class actions. For example, litigation over vulnerabilities and hacks of connected devices, such as cars, medical devices, drones, and any devices that are part of the Internet of Things may be far easier to litigate if all a plaintiff has to show is that a claimed future harm is "plausible . . . to infer." *Attias*, 2017 WL 3254941, at *6. This standard may also encourage lawsuits over claimed misuse of "big data" or pricing algorithms. *See* "Digital Redlining: Increasing Risk of 'Soft Regulation' and Litigation," *Bloomberg BNA Electronic Commerce & Law Report* (June 8, 2016), available here.

Companies that hold consumer data or provide products or services to the public should take notice. The economic incentives and technology impacts of this sort of litigation are immense.

*****

Wiley Rein has worked on data security and cybersecurity for years. We are deeply involved in preparing for the Internet of Things, including considerations about liability. We counsel companies and associations on legal and policy trends, including the effect of litigation on innovation. Several years ago, Megan Brown filed the only amicus brief opposing standing in *Clapper v. Amnesty International*, available here.