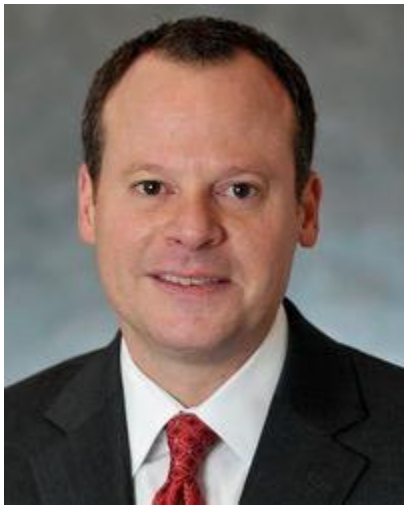
Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Adobe Data Breach Ruling Gives New Hope To Plaintiffs

Law360, New York (September 24, 2014, 9:39 AM ET) --



Michael Buchanan

Data breach class actions have multiplied rapidly in the wake of several sophisticated, large-scale attacks on corporate computer systems, and a recent decision in California federal court may have added some new fuel to the fire. In a sharp departure from a string of recent decisions across the country, Judge Lucy H. Koh of the Northern District of California concluded that plaintiffs suing Adobe Systems Inc. had standing to bring claims against Adobe arising from a massive breach in 2013 even though they could not allege actual misuse of their stolen personal information.

The decision in In re Adobe Systems Inc. Privacy Litigation, No. 13-CV-05226-LHK (N.D. Cal. Sept. 4, 2014), is significant, as most other courts since the U.S. Supreme Court's decision in Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013), have dismissed similar actions for lack of standing where data breach plaintiffs have not alleged actual misuse of their data.

In a series of recent decisions, defendants have successfully relied on Clapper to dismiss data breach class actions, seemingly without regard to the individual facts of each case. The Adobe decision is a reminder that the law remains unsettled in this active area of class action and data security litigation, and appears likely to spur additional lawsuits in California federal court.

In re Adobe Systems arose from a 2013 attack on Adobe's computer network, in which hackers gained unauthorized access to Adobe's servers, including their "Creative Cloud" platform, a subscription-based program where customers pay a monthly fee to access Adobe's products and services. Adobe collects a variety of personal information from its users, including names, email and mailing addresses, telephone numbers, passwords, and credit card numbers and expiration dates for millions of customers.

In July 2013, hackers attacked Adobe's servers and spent several weeks inside Adobe's network without detection. During this sophisticated, weeks-long intrusion, hackers removed gigabytes of customer data and Adobe source code, an intrusion that remained undiscovered until September 2013 when independent security researchers discovered stolen Adobe source code on the Internet. Adobe disclosed the data breach in October 2013, announcing that hackers had accessed personal information belonging to 38 million customers, including names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and email addresses. Adobe also disclosed that hackers were able to decrypt customers' credit card

numbers.

In the wake of the data breach, various plaintiffs whose personal information had been compromised brought actions against Adobe alleging numerous violations of California's Customer Records Act, Calif. Civil Code §§ 1798.81.5 and 1798.82, and seeking injunctive relief under California's Unfair Competition Law, Calif. Bus. & Prof. Code §§ 17200 et seq. Plaintiffs also sought a declaratory judgment that Adobe had breached its contractual obligations to provide reasonable security protection to its customers.

Clapper v. Amnesty International USA: Article III Standing and "Increased Risk of Harm"

Following in the footsteps of other data breach defendants, Adobe moved to dismiss all claims, arguing, among other things, that the plaintiffs lacked standing under Clapper v. Amnesty International USA. Clapper involved a challenge to the Foreign Intelligence Surveillance Act, where various attorneys at public interest and media organizations whose work required them to communicate with individuals outside of the United States argued that they were likely to be the subject of surveillance by the government. They claimed to have suffered injury based on "an objectively reasonable likelihood that their communications [would] be acquired [under FISA] at some point in the future." 133 S. Ct. at 1146.

The respondents in Clapper did not allege that any of their communications actually had been intercepted, or that the government even sought to target them directly. The Supreme Court thus concluded that their fears were "highly speculative" and based on a "highly attenuated" chain of possibilities that did not result in a "certainly impending" injury. Id. at 1148.

Since Clapper, federal courts in Ohio, Illinois, New Jersey and California have dismissed claims, concluding that increased risk of harm resulting from a data breach is insufficient to confer Article III standing. For instance, in In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig. (SAIC), No. 12-347 (JEB) (D.D.C. May 9, 2014), a thief stole encrypted backup data tapes containing personal medical information for over 4 million U.S. military members and their families out of the back of a car. The SAIC court concluded that plaintiffs had suffered no immediate injury because the thief would have needed to identify the tapes, obtain specialized equipment to read them, break the records' encryption, and view their contents with specialized software. The court thus found plaintiffs' injuries to be as attenuated as the chain of events rejected in Clapper.

Similarly, in Polanco v. Omnicell Inc., 988 F. Supp. 2d 451 (D.N.J. 2013), a thief stole a laptop out of a car. The plaintiffs did not allege that the thief targeted the laptop for its data or any actual misuse of their personal information, and were therefore dismissed for lack of standing.

In Galaria v. Nationwide Mutual Insurance, No. 2:13-cv-118 (S.D. Ohio, Feb. 10, 2014), victims of a data breach claimed they suffered harm because they were statistically more likely than the general public to become victims of fraud. The court, citing Clapper, found that the plaintiffs' injury could hardly be "certainly impending" when the harm they feared had "less than a 20% chance of occurring."

Adobe argued that Clapper had implicitly overruled Krottner v. Starbucks Corp., a 2010 Ninth Circuit decision which held that "the possibility of future injury may be sufficient to confer standing" where the plaintiff is "immediately in danger of sustaining some direct injury as the result of the challenged conduct." 628 F.3d 1139, 1142 (9th Cir. 2010). Unlike Clapper, Krottner was a data breach case where a thief stole a laptop from Starbucks containing unencrypted names, addresses and Social Security numbers of approximately 97,000 Starbucks employees.

Judge Koh disagreed with Adobe, holding that Clapper did not abrogate Krottner and did not fundamentally change the law of standing or reformulate "the familiar standing requirements of injury-in-fact, causation, and redressability." Rather, Judge Koh limited Clapper to its unique facts, stating that the Supreme Court "merely held that the Second Circuit had strayed from these well-established standing principles by accepting a too-speculative theory of future injury."

More significantly, Judge Koh concluded that even if Krottner no longer applied, plaintiffs still had standing under Clapper itself because "the risk that Plaintiffs' personal data will be misused by the hackers who breached Adobe's network is immediate and very real." Recognizing that hackers who intruded Adobe's computer systems deliberately targeted Adobe's servers and spent several weeks collecting names, usernames, passwords, email addresses, phone numbers, mailing addresses, and credit card numbers and expiration dates, and that some stolen data had already surfaced on the Internet, Judge Koh concluded that the danger that the plaintiffs' data would be misused was "certainly impending," and that plaintiffs need not wait until they suffer identity theft or credit card fraud in order to have standing.

Ultimately, Judge Koh trimmed some of the plaintiffs' claims, concluding that the plaintiffs had failed to establish any injury traceable to Adobe's failure to timely notify customers of the breach, and that some plaintiffs had not adequately pleaded injury under California's UCL. The court denied the remainder of Adobe's motion to dismiss, and gave the plaintiffs 30 days to file a seconded amended complaint curing the pleading deficiencies identified in the order.

Effect of the Decision

The Adobe decision creates new uncertainty for data breach defendants and raises some hope for class action plaintiffs and their lawyers. Before this opinion, only one other court had ruled that Article III standing exists without allegations of actual misuse of the breached information. See In re Sony Gaming Networks and Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942 (S.D. Cal. Jan 21, 2014).

Judge Koh's decision demonstrates that data breach class actions can move forward even where plaintiffs cannot allege actual misuse of their data, at least in cases involving sophisticated hacker attacks where the intent to misappropriate data is obvious.

In light of the continued proliferation of data breaches, litigation in this area is likely to grow. Although the majority of courts have held that allegations of injury in the absence of misuse of data are insufficient to establish Article III standing under Clapper, the Adobe and Sony decisions are proof that the issue is far from settled.

—By Michael Buchanan, Michelle Cohen and Ben Rossen, Patterson Belknap Webb & Tyler LLP

Michael Buchanan is a partner in Patterson Belknap's New York office and former chief of the Securities and Health Care Fraud Unit at the U.S. Attorney's Office for the District of New Jersey. Michelle Cohen is a partner and Ben Rossen is an associate in the firm's New York office.