THOMSON REUTERS

Westlaw®

Shifting sands: The data breach litigation landscape in 2017

By Kenneth N. Rashbaum, Esq., *Barton LLP*

JUNE 30, 2017

The smiling red skull glowing from the computer monitor is a rather rude indication that your computer or information system has been attacked.

Upon further investigation, you learn that a significant amount of personal, company and other protected data have been hacked.

Can these actions result in a lawsuit that survives a motion to dismiss?

Judges are human beings after all, and the plethora of data breaches in late 2016 and early 2017, from the Democratic National Committee to the CIA, has not gone unnoticed by the judiciary.

The state of the law as to causes of action, standing and damages in litigation arising from data breaches is evolving even faster than the speed of change in technology law as a whole.

This article will discuss the current state of that legal landscape (as of the date of publication, anyway), analyzing common causes of action and trends in defenses concerning standing and questions of damages.

DATA BREACH CLASS ACTIONS: THE STANDING ISSUE

Class action litigation arising from massive data breaches rises or falls, like most other civil litigation, with proof of three elements: fault, causation and damages.

But it's mostly the third element, damages, as it pertains to the existence of standing that determines whether the litigation will survive a motion to dismiss.

Where the injury is exposure or theft of personal electronic information, the criteria for Article III standing — a prerequisite to a federal lawsuit — are, to use a phrase much favored by mountain bikers, "gnarly."

To add to this combustible mix, the federal circuits are split on how, and whether, the loss of personally identifiable digital information is a compensable injury.

The Supreme Court has yet to provide clarity in this area.

Splitting the hairs of terms like "concrete," "imminent" and "impending" may bedazzle English teachers, but they cause headaches for lawyers and their clients — regardless of which side of the litigation they may find themselves on.

These cases have arisen, for the most part, from breaches of credit card, bank or health information that is traceable to an identifiable individual.

A limited number of them have involved some form of identity theft, where the information was used to file false tax returns, open bogus credit card accounts or make online purchases.

But in many of the lawsuits, these harms have not yet occurred.

Is the mere loss of personal, sensitive information sufficiently grievous to confer standing? The decisions answering this question are often highly fact-dependent.

Supreme Court guidance has not been terribly elucidating, and the federal circuit courts have sometimes strained to apply those recent decisions to data breach cases.[1]

The plethora of data breaches in late 2016 and early 2017, from the Democratic National Committee to the CIA, has not gone unnoticed by the judiciary.

The 3rd U.S. Circuit Court of Appeals held in *In re Horizon Healthcare Services Inc. Data Breach Litigation* that loss of personal information is itself a sufficient injury to grant standing.[2]

Nonetheless, the Horizon case does not have a clear path to trial. That is because it was brought under Fair Credit Reporting Act, and it is by no means clear that Horizon, a health insurer, is an entity covered under that statute.

The 6th and 7th circuits have held that potential harm from identity theft is enough to establish standing.[3]

As the 6th Circuit put it so eloquently in *Galaria v. Nationwide Mutual Insurance Co.*, "There is no need for speculation where plaintiffs allege that their data has already been stolen and is now in the hands of ill-intentioned criminals."

Yet, in the 7th Circuit cases that preserved claims stemming from data breaches — at least at the stage of motions to dismiss on the pleadings — plaintiffs had demonstrated tangible injuries in the form of identity theft and fraudulent credit card charges.

The 9th Circuit held such claims to be deserving of standing in *Krottner v. Starbucks Corp.*, but the 4th Circuit, in *Beck v. MacDonald*, held that the risk of identity theft was merely a "speculative threat."[4]

Further clarification from the Supreme Court may be in order. On the other hand, the fact that these cases are heavily fact-dependent may lead the Supreme Court to take a hands-off approach despite the epidemic of massive data breaches.

In the meantime, plaintiffs should scrutinize these decisions and consider how they can frame their injuries to allege more than generalized, speculative threats.

Defendants can aver that the facts of the specific claims at issue are ethereal and that there is no compensable injury.

STATE STATUTORY, COMMON LAW AND REGULATORY ACTIONS

Organizations at risk for data breach — essentially all organizations that create, host or transfer large columns of personal data — ignore state laws at their peril.

Health insurer Anthem Inc. faces a multidistrict class action in the U.S. District Court for the Northern District of California over a cyberattack that compromised its systems from December 2014 until January 2015, allegedly affecting about 80 million policyholders.

Despite the federal venue, the claims at issue involve consumer protection statutes from New York, California and Kentucky.

The court denied motions to dismiss state law claims that alleged material misrepresentations about security practices in consumer-oriented contracts.[5]

State common law claims will continue to loom large in data breach litigation as well, as their "legs" may be on less perilous terrain in state court than they are in federal court.

In *Mott v. Nassau University Medical Center,* a claim for violation of a patient's medical privacy withstood a motion to dismiss on the pleadings.[6]

The motion was based, in part, on a refusal on the part of the Office for Civil Rights of the U.S. Department of Health and Human Services to bring a penalty proceeding under the Health Insurance Portability and Accountability Act.

The defendant alleged the doctrine of collateral estoppel barred the plaintiff's claim, but the court held that the Office for Civil Rights did not rule on New York's common law fiduciary obligation on the part of a medical provider to keep a patient's information confidential.

Similarly, in *Pierre-Paul v. ESPN*, the court declined to dismiss a case in which the medical records of New York Giants defensive end Jason Pierre-Paul were photographed, sent to ESPN and then broadcast.[7]

The court denied the motion to dismiss on the ground that state negligence common law permitted a violation-of-privacy claim.

The *Pierre-Paul* case, which was later settled, shows the availability and potential impact in cybersecurity litigation of a negligence cause of action.

Viewed broadly, negligence is a departure from a standard of care.

Newer malware variants are capable of turning computers, networks and even internet-connected devices such as baby video cameras and home routers into a botnet, which is a network of computers and devices linked by malware into a type of supercomputer capable of wreaking great havoc.

This occurred in the October 2016 attack on domain name system provider Dyn Inc., which brought much of the e-commerce on the East Coast to a screeching halt.

Affected individuals and organizations may have causes of action against device owners who did not take reasonable steps to secure the devices so as to prevent other computers and networks from being compromised by being drawn into a botnet.[8]

> The state of the law as to causes of action, standing and damages in litigation arising from data breaches is evolving even faster than the speed of change in technology law as a whole.

In the absence of wide-reaching cybersecurity legislation at the federal level, states will take a more aggressive role in security regulation and enforcement and will undoubtedly bring actions to enforce those regulations.

New York

New York state has implemented cybersecurity regulations, effective March 1 for organizations supervised by the state's Department of Financial Services.

These regulations will require significant information management changes. Because New York is the nation's financial capital, these regulations may be a template for other states with regard to financial services cybersecurity.

The New York Department of Financial Services supervises, and the regulations apply to, banks, New York offices of foreign banks, credit unions, holding companies, insurers (including health insurance carriers), insurance brokers and certain investment companies.

New York Attorney General Eric Schneiderman has shown little reluctance to pursue data breach actions, having announced on March 23 that his office had obtained settlements with a number of mobile health applications

developers for, among other things, failing to disclose how they release health information obtained through the applications.[9]

Massachusetts

Massachusetts has had regulations that protect the personal information of its residents for many years, and its attorney general has brought actions pursuant to them.[10]

California

In February 2016, the California attorney general's office issued a "California Data Breach Report" in which then-Attorney General Kamala Harris stated that the document "CIS Controls for Effective Cyber Defense," which comprises 20 separate cybersecurity controls, would be the "minimum standard for cybersecurity in the state."[11]

It is likely that other states will follow the lead of New York, Massachusetts and California. State regulatory actions, including litigation, will be an increasingly prominent feature of the data breach landscape in 2017 and beyond.

This is a particularly strong trend in light of recent action by the Trump administration to roll back federal regulations on internet privacy.

As The New York Times reported March 27 with regard to state legislative initiatives to fill a perceived federal vacuum in privacy and security protection: "Online privacy is the rare issue that draws together legislators from the left and the right. At the state level, anyway, some of the progress has come from a marriage between progressive Democrats and libertarian-minded Republicans, who see privacy as a bedrock principle."[12]

WAITING IN THE WINGS: SHAREHOLDER DERIVATIVE ACTIONS

Significant change in data breach liability analysis may also be afoot in shareholder derivative claims stemming from massive data breaches — particularly where the actions of the organization may have violated state cybersecurity laws.

The business-judgment rule, which generally protects corporate directors from the consequences of decisions made in the best interest of the corporation, has been eroded by two recent decisions in data breach cases.

The U.S. District Court for the District of New Jersey dismissed a shareholder's action stemming from the Wyndham Worldwide Corp. data breach in *Palkon v. Holmes*.[13]

The court said the directors earned the protection of the business judgment rule by taking a number of steps to investigate and remediate the breach and its consequences.

Reinforcing a trend that the rule is not absolute when it comes to data breach liability, the Delaware Chancery Court wrote in *Reiter v. Fairbank* that an action may lie where there is evidence that board action or inaction violates cybersecurity laws or regulations, or where a board's failure to implement controls over electronic information violates state law.[14]

Significantly, the court distinguished, for purposes of a motion to dismiss based on the business judgment rule, business decisions made by the board (which will be, for the most part, cloaked by the rule), and compliance decisions (which are entitled to lesser protection).

> State common law claims will continue to loom large in data breach litigation as well, as their "legs" may be on less perilous terrain in state court than they are in federal court.

Forty-eight states have some form of data privacy or security laws or regulations (ranging from breach notification statutes to the strict proscriptions of the New York and California regulations). For this reason it is only a matter of time before a court permits a derivative action based on a data breach to proceed to trial.

CONCLUSION

Judges, like state legislators, send and receive email, shop online and otherwise browse the internet. Like the rest of us, they are vulnerable to data breaches.

Traditional rules on standing have been relaxed recently with regard to data breaches, and it is likely more, rather than fewer, claims arising from data breaches will be permitted to proceed in step with the increase in the number and size of cyberattacks and data breaches.

It is a good idea for organizations in e-commerce and others who host large volumes of data to review their insurance coverage with regard to such exposures — and to set aside time and resources to revisit and, where necessary, update safeguards for protected data.

NOTES

[1] The analysis begins with the decision in *Clapper v. Amnesty Int'l USA,* 568 U.S. 398 (2013), where the Supreme Court ruled that alleged future harm may be compensable so long as it is "certainly impending." Most recently, writing for the majority in *Spokeo Inc. v. Robins,* 136 S. Ct. 1540 (2016), Justice Samuel Alito Jr. wrote that a statutory violation may provide "particularization" of injury but not necessarily "concreteness." He qualified this statement by writing that concreteness does not necessarily require that the alleged injury be "tangible." He also said real risk of harm may satisfy the concreteness requirement. The high court remanded the case to the 9th U.S. Circuit Court of Appeals for such a determination.

[2] 846 F.3d 625 (3d Cir. 2017). The panel distinguished *Spokeo* on the ground that *Spokeo* did not involve information protected by a federal statute such as the Health Insurance Portability and Accountability Act.

[3] *Galaria v. Nationwide Mut. Ins. Co.,* 663 Fed. Appx. 384 (6th Cir. 2016); *see also Remijas v. Neiman Marcus Grp. LLC,* 794 F.3d 688 (7th Cir. 2015) and *Lewert v. P.F. Chang's China Bistro Inc.,* 819 F.3d 963 (7th Cir. 2016), respectively.

[4] 628 F.3d 1139 (9th Cir. 2010); 848 F.3d 262 (4th Cir. 2017). Admittedly, the 9th Circuit's decision is a pre-*Clapper* case, though it has not been overruled or distinguished in a meaningful way.

[5] 162 F. Supp. 3d 953 (N.D. Cal. 2016).

[6] No. 600052/11, 2011 WL 4657387 (N.Y. Sup. Ct., Nassau Cty. Sept. 16, 2011).

[7] No. 16-cv-21156, 2016 WL 4530884 (S.D. Fla. Aug. 29, 2016).

[8] Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage,* WIRED, Oct. 21, 2016, http://bit.ly/2efBbRT.

[9] Press Release, N.Y. State Attorney Gen., A.G. Schneiderman Announces Settlements with Three Mobile Health Application Developers for Misleading Marketing and Privacy Practices (Mar. 23, 2017), http://on.ny.gov/2o9lYBj; *see also* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.00.

[10] 201 MASS CODE REGS. 17.01; Press Release, Mass. Attorney Gen., Women & Infants Hospital to Pay $150,000 to Settle Data Breach Allegations Involving Massachusetts Patients (July 23, 2014), http://bit.ly/2qTEhQu.

[11] Kamala D. Harris, Cal. Dep't of Justice, California Data Breach Report (2016), http://bit.ly/2rti8Hv.

[12] Conor Dougherty, *Push for Internet Privacy Rules Moves to Statehouses,* N.Y. TIMES, Mar. 26, 2017, http://nyti.ms/2nXNrd8.

[13] No. 14-cv-1234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

[14] No. CV 11693, 2016 WL 6081823 (Del. Ch. Oct. 18, 2016).

This article first appeared in the June 30, 2017, edition of Westlaw Journal Computer & Internet.

ABOUT THE AUTHOR

Kenneth N. Rashbaum heads the privacy and cybersecurity practice group at **Barton LLP** in New York, where he is a partner. He is also an adjunct professor at Fordham Law School. He can be reached at krashbaum@bartonesq.com.