Don't Be a Plaintiff's Lawyer's Next Victim

Avoiding the Pitfalls of Data Breach Litigation

By Leon Silver, Andy Castricone, and Christina Vander Werf

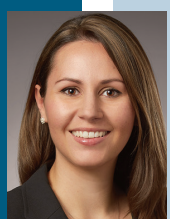
Keeping up to date on the yet-unresolved dynamic of evolving case law in data breach litigation is imperative.

Data breaches and their resulting costs are both on the rise. While Verizon dubbed 2013 the "year of the retailer breach," the trend continued in 2014 with a number of major, high-profile cyber-attacks against retailers. Verizon Enterprise Solutions, 2014 Data Breach Investigations Report 3. The importance of risk assessment and data security is growing, even for those who don't already know that the average cost of a data breach for U.S. companies is $5.85 million. Ponemon Institute LLC, 2014 Cost of Data Breach Study: Global Analysis 6. For many large retailers, the costs are substantially higher. For example, Neiman Marcus recently reported that it incurred $12.6 million in expenses relating to its 2013 data breach. Neiman Marcus Group LTD LLC, Quarterly Report (Form 10-K) 39 (Sept. 25, 2014). Target has incurred a staggering $236 million in expenses since its data breach in the fourth quarter of 2013. Target Corp., Quarterly Report (Form 10-Q) 9 (Aug. 27, 2014). This amount does not account for the potential liability or the potential settlement in the pending class action. *See In re Target Corp. Customer Data Security Breach Litigation*, No. 0:14-md-02522 (D. Minn. filed Apr. 2, 2014).

So what's a retailer to do? Aside from undertaking the measures needed to prevent data breaches and periodically updating those controls, retailers can help limit their exposure in litigation stemming from a data breach by understanding plaintiffs' constantly evolving means of attack.

This article aims to assist retailers and defense attorneys in that task by examining the evolving strategies of the plaintiffs' bar, reconciling competing court rulings, and offering logistically practical suggestions to implement as part of your data governance program.





■ Leon Silver and Andy Castricone are partners of Gordon & Rees LLP in the Phoenix and San Francisco offices, respectively. Mr. Silver is co-chair of the Cybersecurity Specialized Litigation Group of the DRI Commercial Litigation Committee and co-chair of the Commercial Litigation Specialized Litigation Groups of the DRI Retail and Hospitality and Commercial Litigation committees. Mr. Castricone serves as the firm's national practice group leader for privacy and data security. Ms. Vander Werf, an associate who represents clients throughout southern California and Arizona, is a member of the commercial litigation and privacy and data security practice groups. She is also the Community Chair of the Cybersecurity SLG of DRI's Commercial Litigation Committee.

Data Breach Litigation and Traditional Notions of Injury

Data breaches, and their accompanying lawsuits, are nothing new. For the better part of a decade, courts have been grappling with whether plaintiffs who allege an increased risk of harm stemming from a data breach have standing to sue under Article III of the U.S. Constitution.

Pisciotta v. Old National Bancorp, 499 F.3d 629 (7th Cir. 2007), involved a hacker who obtained access to the confidential information of tens of thousands of Old National Bancorp site users. Individuals whose information was accessed filed suit, seeking compensation for past and future credit monitoring services. The Seventh Circuit noted that many district courts had "concluded that the federal courts lack jurisdiction because plaintiffs whose data has been compromised, but not yet misused, have not suffered an injury-in-fact sufficient to confer Article III standing." *Pisciotta*, 499 F.3d at 634 (citing *Randolph v. ING Life Ins. & Annuity Co.*, 486 F.Supp.2d 1, 10 (D.D.C. 2007); *Bell v. Axciom Corp.*, 2006 U.S. Dist. LEXIS 72477, 2006 WL 2850042, at *2 (E.D. Ark. Oct. 3, 2006); *Key v. DSW, Inc.*, 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006); *Giordano v. Wachovia Sec., LLC*, 2006 U.S. Dist. LEXIS 52266, 2006 WL 2177036, at *5 (D.N.J. July 31, 2006)). The court adopted a contrary view, holding that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions." *Pisciotta*, 499 F.3d at 634.

The Ninth Circuit followed suit several years later in *Krottner v. Starbucks Corporation*, 628 F.3d 1139 (9th Cir. 2010). In *Krottner*, a thief stole a laptop from Starbucks that contained the unencrypted names, addresses, and Social Security numbers of approximately 97,000 Starbucks' employees. The plaintiffs alleged that they were at an increased risk of future identity theft as a result of the theft. In analyzing whether an increased risk of future harm was sufficient to confer standing, the court noted, "[i]f a plaintiff faces 'a credible threat of harm' and that harm is 'both real and immediate, not conjectural or hypothetical,' the plaintiff has met the injury-in-fact requirement for standing under Article III." *Krottner*, 628 F.3d at 1143 (internal citations omitted). Given the facts at hand, the Ninth Circuit concluded that the plaintiffs had alleged a credible threat of real and immediate harm stemming from the theft of the laptop. Had the allegations been more conjectural or hypothetical, such as a risk that the laptop would be stolen in the future, that would have been insufficient to confer standing. *Id.*

Similarly, the First Circuit adopted *Krottner*'s reasoning when finding that a plaintiff had failed to allege an injury that would confer standing. *Katz v. Pershing, LLC*, 672 F.3d 64 (1st Cir. 2012). The plaintiff alleged that her brokerage account information was vulnerable to prying eyes because it was being inadequately protected by the defendant's system. The plaintiff did not allege that there had been any unauthorized access or misuse of her information. The court concluded that the omission of such allegations was "fatal" and that the plaintiff could not satisfy "Article III's requirement of actual or impending injury." *Katz*, 672 F.3d at 80.

The Supreme Court Creates an "Out": *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013)

In 2013, defense attorneys gained a new weapon in their arsenal: *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013). *Clapper* involved Section 702 of the Foreign Intelligence Surveillance Act of 1978, codified at 50 U.S.C. §1881a (2006), which allows the U.S. attorney general and the director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not "United States persons" and are reasonably believed to be located outside the United States. The respondents were "United States persons" whose work allegedly required them to engage in sensitive international communications with individuals who are likely targets of §1881a surveillance. The respondents sought a declaration that §1881a was unconstitutional, as well as an injunction against §1881a surveillance.

The district court determined that the respondents lacked Article III standing. On appeal, the Second Circuit reversed. It agreed with the respondents that they had standing due to the objectively reasonable likelihood that their communications would be intercepted at some point in the future. It also agreed that the respondents had present injuries in fact that stemmed from a reasonable fear of future harmful government conduct.

The Supreme Court reversed, reiterating the principle that "'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." *Clapper*, 133 S. Ct. at 1147 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158, 110 S. Ct. 1717, 109 L.Ed.2d 135 (1990) (emphasis added)). The respondents' threatened injury was "highly speculative" and relied on a "highly attenuated chain of possibilities." *Id.* at 1148. For the threatened injury to become an actual injury required finding the following conditions: (1) the government would have to target the non-U.S. persons with whom the respondents communicate, (2) the government would have to invoke the authority of §1881a, (3) the judges who serve on the Foreign Intelligence Surveillance Court would have to conclude that the proposed surveillance satisfied the §1881a safeguards, (4) the government would have to successfully inter-

The court adopted a contrary view, holding that "the injury-in-fact requirement can be satisfied by a threat of future harm or by an act which harms the plaintiff only by increasing the risk of future harm that the plaintiff would have otherwise faced, absent the defendant's actions."

cept the communications of respondents' contacts, and (5) the respondents would have to be parties to the particular communications intercepted. *Id.*

Likewise, the respondents could not claim an injury in fact, and thereby standing, by voluntarily undertaking costly and burdensome measures to protect the confidentiality of their communications, such as traveling abroad to speak to their contacts in person. *Clapper*, 133 S. Ct. at 1151. In short, the Court reasoned that the "respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Id.*

The Supreme Court reversed, reiterating the principle that "'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient."

Clapper Progeny Leads to Routine Dismissals of Data Breach Cases

Within months, defense attorneys began using *Clapper* to challenge class action suits arising from data breach incidents. In September 2013, the U.S. District Court for the Northern District of Illinois dismissed a class action complaint against Barnes & Noble. *In re Barnes & Noble Pin Pad*, No. 12-cv-8617, 2013 U.S. Dist. LEXIS 125730, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013). In that case, skimmers potentially stole customer credit and debit information from 63 locations in nine states. The plaintiffs alleged a variety of injuries, including an increased risk of identity theft or fraud, and time and expense relating to mitigating this increased risk. Relying on *Clapper*, the court determined that these alleged damages were insufficient to confer standing to the plaintiffs partly because "speculation of future harm does not constitute actual injury." *In re Barnes & Noble Pin Pad*, 2014 U.S. Dist. LEXIS 125730, at *12. Further, "[p]laintiffs 'cannot manufacture standing by incurring costs in anticipation of non-imminent harm." *Id.* at *11–*12 (quoting *Clapper*, 133 S. Ct. at 1151).

Again in *Hilary Remijas et al. v. The Neiman Marcus Group LLC*, 1:14-cv-01735, 2014 U.S. Dist. LEXIS 129574, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014), the U.S. District Court for the Northern District of Illinois relied on *Clapper* to dismiss a class action complaint filed against Neiman Marcus. *Remijas* involved the potential disclosure of 350,000 Neiman Marcus customers' payment card data and personally identifiable information. Of the cards that may have been affected, at least 9,200 were subsequently used fraudulently elsewhere. The plaintiffs in *Remijas* were among those 9,200. Similar to the plaintiffs in *In re Barnes & Noble Pin Pad*, they alleged an increased risk of future fraudulent credit card charges, an increased risk of identity theft, and losses of time and money associates with these risks.

The court noted that "[a]llegations of future potential harm may suffice to establish Article III standing, but the future harm must be 'certainly impending.'" *Remijas*, 2014 U.S. Dist. LEXIS, at *4. In that vein, the court recognized that there was a "certainly impending" risk that the plaintiffs, and others whose information was disclosed, would see similar fraudulent charges appear on their credit card statements as a result of the cyber-attack. However, that was still insufficient to confer standing to the plaintiffs because the injury still needed to be *concrete*. As there was no allegation that the plaintiffs were financially responsible for the unauthorized charges, the alleged injuries were not concrete and could not confer Article III standing. *Remijas*, 2014 U.S. Dist. LEXIS, at *8–*9.

As in *In re Barnes & Noble Pin Pad*, the court rejected the argument that the time and the money spent mitigating the risk of future fraud and identity theft was not sufficient to confer standing; "The cost of guarding against a risk is an injury sufficient to confer standing only if the underlying harm the plaintiff is seeking to avoid is itself a cognizable injury." *Remijas*, 2014 U.S. Dist. LEXIS, at *11.

More Recent Departures from *Clapper* and New Standing Analysis

Although *Clapper* was used successfully in several data breach cases, courts have more recently split on its implementation. The first case to do so was *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942 (S.D. Cal. 2014). In *Sony*, the plaintiffs' personal and financial information was accessed through gaming consoles. The plaintiffs alleged that the wrongful disclosure of their personal information increased the risk of future harm. Sony challenged the plaintiffs' standing based on *Clapper*.

The U.S. District Court for the Southern District of California disagreed with Sony that *Clapper* tightened the injury-in-fact analysis. *Clapper* used different language than other cases, but it did not create a new Article III framework. *Sony*, 996 F. Supp. 2d at 961. The court found "both *Clapper* and *Krottner* controlling, and case law in this circuit analyzing the 'injury-in-fact' requirement following *Krottner* highly persuasive." *Id.* at 961. The court further noted that courts in the Ninth Circuit "have routinely denied motions to dismiss based on Article III standing where a plaintiff alleges that his personal information was collected and then wrongfully disclosed." *Id.* at 962 (citing *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011); *Doe 1 v. AOL, LLC*, 719 F. Supp. 2d 1102 (N.D. Cal. 2010); *San Luis & Delta-Mendota Water Auth. v. U.S. Dep't of the Interior*, 905 F. Supp. 2d 1158 (E.D. Cal. 2012)). The court ruled consistently with these cases, finding that "Plaintiffs' allegations that their Personal Information was collected by Sony and then wrongfully disclosed as a result of the intrusion [was] sufficient to establish Article III standing." *Sony*, 996 F. Supp. 2d at 962.

Following in *Sony*'s footsteps, the U.S. District Court for the Northern District of Illinois found that the plaintiffs' allegations of elevated risk of identity theft were sufficient to confer Article III standing. *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, 2014 WL 3511500 (N.D. Ill. July 14, 2014) (dis-

missed for failure to state a claim). In *Moyer*, malware attacked point-of-sale systems containing customers' payment card numbers and expiration dates. Approximately 2.6 million credit or debit cards were affected by the breach. In analyzing whether the plaintiffs had Article III standing, the court distinguished *Clapper* "based on its admittedly rigorous application of the 'certainly impending' standard in a case that involved (1) national security and constitutional issues and (2) no evidence that the relevant risk of harm had ever materialized in similar circumstances." *Moyer*, 2014 U.S. Dist. LEXIS 96588, at *19. Instead, the court followed *Pisciotta*'s holding that an elevated risk of identity theft is a cognizable injury in fact.

Similarly, the U.S. District Court for the Northern District of California held that pleading an increased risk of harm arising from a data breach is sufficient to confer standing. *In re Adobe Systems Inc. Privacy Litigation*, No 13-cv-05226-LHK, 2014 U.S. Dist. LEXIS 124126, 2014 WL 4379916 (N.D. Cal. Sept. 4, 2014). In *Adobe*, hackers gained unauthorized access to Adobe's servers and spent weeks inside the network removing personal and financial information for 38 million customers. The hackers also used Adobe's systems to decrypt customers' credit card numbers, which had been stored in an encrypted form. The plaintiffs alleged that as a result of the breach, they were at an increased risk of future harm and incurred, or would incur, costs to mitigate this increased risk. Consistent with *Sony*, the court concluded that "*Clapper* did not change the law governing Article III standing. The Supreme Court did not overrule any precedent, nor did it reformulate the familiar standing requirements of injury-in-fact causation, and redressability." *Adobe*, 2014 U.S. Dist. LEXIS 124126, at *24. Also, as in *Moyer*, the court noted that "*Clapper*'s discussion of standing arose in the sensitive context of a claim that other branches of government were violating the constitution, and the U.S. Supreme Court itself noted that its standing analysis was unusually rigorous as a result." *Id.* at *25.

The *Adobe* decision went even further concluding that even if *Krottner* was no longer good law, the threatened harm was sufficiently concrete and imminent to satisfy *Clapper*. Unlike *Clapper*, in which the claims of future harm rested on a chain of events that was highly attenuated and highly speculative, the risk that plaintiffs' personal data would be misused by the hackers who breached Adobe's network was immediate and very real. *Adobe*, 2014 U.S. Dist. LEXIS 124126, at *27. The decision reasoned that "to require Plaintiffs to wait until they actually suffer identity theft or credit card fraud in order to have standing would run counter to the well-established principle that harm need not have already occurred or be 'literally certain' in order to constitute injury-in-fact." *Id.* at *28.

Are *Sony* and *Adobe* Anomalies or Do They Reflect a Trend?

It's too early to know if *Sony*, *Moyer*, and *Adobe* represent a changing tide in the prosecution of data breach claims. The U.S. District Court for the Northern District of Illinois has already indicated that *Moyer* may be an outlier in its district. *See Remijas*, 2014 U.S. Dist. LEXIS 129574, at *4–*5. Nonetheless, the plaintiffs in *Lewert v. PF Chang's China Bistro, Inc.*, No. 1:14-cv-04787 (N.D. Ill. filed June 25, 2014), filed in the same district, still cited both *Sony* and *Adobe* in their opposition to PF Chang's motion to dismiss the class action complaint. The court has yet to rule on the motion to dismiss.

Another case to watch relating to a retail data breach is *Solak et al. v. The Home Depot, Inc.*, No. 1:14-cv-02856-WSD (N.D. Ga. filed Sept. 4, 2014). The Home Depot filed a motion to dismiss, claiming that the plaintiffs lack standing under *Clapper*. The plaintiffs will likely rely on *Sony* and *Adobe* in their opposition. The rulings in both cases will be illuminating and should be followed closely by those with an interest in this area of the law.

Plaintiffs Have Found Other Means of Avoiding *Clapper*

Plaintiffs have found other means of avoiding *Clapper*. For example, in *In re LinkedIn User Privacy Litigation*, No 5:12-cv-03088 (N.D. Cal. filed June 15, 2012) (Second Amended Complaint filed Apr. 30, 2013), rather than arguing an increased risk of harm, the plaintiff established Article III standing by alleging that she purchased LinkedIn's premium subscription in reliance on LinkedIn's representation in its User Agreement and Privacy Policy that it was using industry standard protocols and technology to protect data. *See* Order Granting in Part and Denying in Part Defendant's Motion to Dismiss, *In re LinkedIn User Privacy Litigation*, No 5:12-cv-03088 (N.D. Cal. March 28, 2014).

In short, the Court reasoned that the "respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending."

Lately, initiations of suits by financial institutions against companies that experience data breaches have increased. For instance, a credit union filed suit against The Home Depot alleging that as a result of the breach referred to above, it had to, or would have to do the following:

- Cancel or reissue any access device affected by breach;
- Close any deposit, transaction, checking, or other accounts affected by the breach, including stopping payments or blocking transactions with respect to the accounts;
- Open or reopen any deposit, transaction, checking, or other accounts affected by the breach;
- Refund or credit any cardholder to cover the cost of any unauthorized transaction relating to the breach;
- Notify cardholders affected by breach;
- Respond to a higher volume of cardholder complaints, confusion and concern; and

Data Breach, continued on page 64

Data Breach, from page 41

- Increase fraud monitoring efforts.

The credit union also claims that it had already incurred costs for cancelling and reissuing numerous debit cards for its customers affected by the breach. *See First Choice Federal Credit Union v. The Home Depot, Inc.*, No. 1:14-cv-02975 (N.D. Ga. filed Sept. 16, 2014). *See also* Consolidated Class Action Complaint, *In re Target Corp. Customer Data Security Breach Litigation*, No. 0:14-md-02522 (D. Minn. Aug. 1, 2014) (alleging financial institutions suffered damages such as the cost of reissuing cards and reimbursing fraudulent charges).

Shareholders also have started to file suit against companies' officers and directors as a result of these cyber-attacks. As with financial institutions, shareholders can point to tangible harm suffered, as opposed to an increased risk of harm or fully reimbursed losses. For example, in *Mary Davis, et al. v. Gregg W. Steinhafel, et al.*, the plaintiffs alleged that officers and directors of Target breached fiduciary duties owed to the company by failing to protect customers' personal and financial information. As a result, Target incurred substantial costs and suffered lost profits. *See* Verified Consolidated Shareholder Derivative Complaint for Breach of Fiduciary Duty and Waste of Corporate Assets, *Mary Davis, et al. v. Gregg W. Steinhafel, et al.*, No. 0:14-cv-00203 (D. Minn. July 18, 2014).

Conclusion

As with other areas of law, plaintiffs' attorneys practicing in the cyber field are smart and creative, and they have already come up with several different ways to attack a company that has suffered a breach. In the as yet-unresolved dynamic of evolving case law, they quickly develop new angles and arguments as their efforts are hindered or thwarted.

In this ever-changing litigation landscape, only one thing is certain: Where there's a breach, plaintiffs' attorneys are sure to follow. As a result, in addition to developing, implementing, and maintaining a sound data privacy program, retailers need litigation counsel to be part of their breach response teams to help investigate the possibility or probability of any real harm to the data holders. It is not prudent for a company to wait until it has experienced a breach and has become victim to a clever and opportunistic plaintiffs' attorney. Retailers must take proactive steps and learn how to assess risk and protect their companies now—both from a breach or data loss and the litigation that will almost certainly follow. FD