Legal Backgrounder

Vol. 29 No. 2 February 7, 2014

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

Targeting Harm From A Breach:
Plaintiffs' Lawyers Get Creative In Data Privacy Suits

by Robert M. McKenna and Scott Lindlaw

One day after retailer Target confirmed hackers had penetrated its computer systems, compromising the personal information of up to 110 million people, the company offered customers free credit-monitoring services and identity-theft insurance. With consumers' trust on the line, Target sought to reassure them it would protect vulnerable personal data by enlisting an outside service to watch for fraudulent activity.

There was more to Target's offer, five days before Christmas, than holiday altruism or crisis-management. Target could anticipate an avalanche of data-privacy lawsuits claiming, among other things, damages stemming from the cost of individuals buying such services. Plaintiffs' attorneys have been energized by a recent federal appellate court finding that a consumer who reasonably responds to a data breach by purchasing identity-theft insurance (or taking similar protective steps) has been "harmed" merely by incurring that expense.[1] Indeed, a review by the authors of a dozen data-privacy class-action suits filed against Target following the breach showed that each suit identified credit-monitoring expenses as a basis for damages.

By providing these services free of charge, Target could deprive plaintiffs of one claim of "harm."

Target's offer was the latest in the cat-and-mouse legal game playing out between breached companies and the plaintiffs' lawyers who invariably and instantaneously go after them. Five years ago in a Washington Legal Foundation (WLF) Legal Opinion Letter, Professor Raymond T. Nimmer predicted a wave of data-privacy litigation, and questioned whether the suits would founder on the issue of injury or harm.[2] The Target class actions underscore Nimmer was right on both counts, and illustrates the creative new theories plaintiffs' lawyers are developing to show "injury."

In 2012, at least 44 million records were compromised in 621 confirmed data breaches globally.[3] In California alone, 2.5 million people experienced breaches of their Social Security numbers, credit card and bank accounts, and other sensitive information through 131 data breaches.[4] The resulting litigation trend is growing because plaintiffs' lawyers are increasingly savvy and aggressive in exploiting state and federal law. A recent survey of corporate counsel nationwide indicated nearly half anticipate growth in consumer fraud and privacy class actions, versus 15 percent a year earlier; the companies spend an average of $3.3 million defending class actions of all types.[5] A conference of class-action lawyers held last year to share lessons learned from the first wave of privacy-related suits, and to hone new strategies, is another clear signal that such litigation will continue.[6]

Yet Professor Nimmer also presciently questioned whether plaintiffs could establish actual harm in such cases. And as noted on WLF's blog, *The Legal Pulse*, for this reason courts have not been very receptive to these lawsuits.[7] Companies have defended themselves through a variety of methods, often winning dismissal of the cases in the early stages. One fundamental problem plaintiffs face is proving they were injured by a company's data collection methods, or even by a breach. This requirement of injury trips

---

Robert M. McKenna is a partner, and **Scott Lindlaw** is an associate, in the Seattle and Silicon Valley offices, respectively, of the law firm Orrick, Herrington & Sutcliffe LLP. Mr. McKenna was Attorney General of Washington from 2005 to 2013, and serves on Washington Legal Foundation's Legal Policy Advisory Board.

up plaintiffs as they try to establish standing in federal court, and as they seek to prove they have suffered a cognizable injury, i.e., harm for which the jurisdiction will grant relief.

To show standing under Article III of the U.S. Constitution, a plaintiff must establish "an injury-in-fact" that is "concrete and particularized."[8] For years, the "injury-in-fact" requirement was defendants' reliable bulwark against data-privacy suits, resulting in the dismissal of the vast majority of these actions because plaintiffs could not prove concrete injury from privacy "invasions" such as the lost value of information gathered by cookies. The majority of courts continue to reject most of the injury-in-fact theories plaintiffs have advanced. For example, most courts have turned aside claims that data breaches injured plaintiffs merely by increasing the *risk* of identity theft, or elevating plaintiffs' *fear* of such theft.[9] Courts have also carefully restricted *threatened* injury. A 2013 U.S. Supreme Court decision in a government surveillance case required that to meet the "injury-in-fact" requirement of standing, plaintiff must show a threatened injury is at least "certainly impending."[10] That requirement is likely to ripple into the data-privacy litigation realm.[11]

Most courts have also rejected injuries purportedly stemming from data breaches such as emotional distress, increased risk of junk mail, time and effort to respond to the breach, the lost data's intrinsic property value and—yes—the cost of monitoring one's credit.[12]

But this legal landscape is complex and shifting. For example, the First Circuit, the same court that rejected credit-monitoring costs in *Katz v. Pershing*, allowed plaintiffs in another case, *Anderson v. Hannaford Bros. Co.*, to recover for identity-theft insurance and other "mitigation damages" including, apparently, credit-monitoring.[13] The *Katz* court distinguished the cases by observing that in *Anderso*n, "confidential data actually ha[d] been accessed through a security breach and persons involved in that breach have acted on the ill-gotten information."[14] In *Katz*, by contrast, the plaintiff's cause of action was "conjectural" because it rested "entirely on the hypothesis that at some point an unauthorized, as-yet unidentified, third party might access her data and then attempt to purloin her identity," the court found.[15] (Another difference is that in *Katz*, the First Circuit was evaluating whether plaintiffs had standing by virtue of an injury-in-fact; in *Anderson*, the appeals court undertook a related but slightly different inquiry into whether plaintiffs' mitigation costs constituted cognizable harms for which the plaintiff could recover damages under Maine's laws of negligence or implied contract.)

Meanwhile, new "injury" theories recently have gained traction in some courts. One court found injury-in-fact where defendants' collection of location data took a heavy toll on the battery life of plaintiffs' smart phones.[16] And to evade the "injury-in-fact" requirement entirely, plaintiffs also have gravitated recently to federal and state laws containing statutory damages provisions. These statutes set forth damage awards, which take the damage determination out of judges' hands. Indeed, these laws require no evidence of actual injury. Federal statutes such as the Electronic Communications Privacy Act (which includes the Stored Communications Act and the Wiretap Act[17]) and the Video Privacy Protection Act,[18] along with many state laws, specify statutory damages for each violation.

In a key Ninth Circuit case, *Jewel v. NSA*, the plaintiff asserted no specific injury from surveillance devices attached to AT&T's communications network. Yet, the court found that violations of federal surveillance statutes represented injuries-in-fact because "a concrete 'injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.'"[19] In a separate case, *Edwards v. First Am. Corp.*, the same court quoted the same language in finding a plaintiff had standing in a property dispute involving alleged violations of the federal Real Estate Settlement Procedures Act of 1974.[20] The Supreme Court granted certiorari in *Edwards*, but then announced it had improvidently done so and dismissed the action.[21] This withdrawal of certiorari led some commentators to theorize that the Supreme Court tacitly endorses such broad conceptions of standing based on violations of statutes.[22]

Increasingly, companies are trying to stay out of the data privacy class-action game altogether by revising their privacy policies to include provisions that purportedly require consumers to waive their right to join such actions in favor of binding arbitration.[23] This approach may have received a boost with the U.S. Supreme Court's landmark decision in *AT&T Mobility LLC v. Concepcion,*[24] which invalidated a California rule barring class-action waivers in the context of consumer contracts.

Target, of course, is no longer on the sidelines. It faces dozens of class-action lawsuits in federal courts from coast to coast. A review by the authors of a dozen of the complaints stemming from the breach[25] shows that a small minority appear able, on the face of the pleadings, to show injury-in-fact that is "concrete and particularized." For example, Scott G. Savedow, the named plaintiff in *Savedow v. Target Corp*., alleges that "[a]s a result of the Data Breach, Plaintiff's Personal information was stolen, he directly suffered from identity theft and fraud, and is exposed to future and likely ongoing fraud as well."[26] The complaint provides a detailed account of fraudulent transactions Savedow alleges stemmed from the Target breach, including a chart showing purported unauthorized ATM withdrawals from his bank account.[27]

Most of the other complaints, however, are vague, straining to show the kind of injury-in-fact required to get the plaintiffs past the standing hurdle.[28] One makes this curious claim:

> A portion of the services purchased from Target by Plaintiff and the Class necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of [personally identifiable information], including their credit card information. Because Plaintiff and the Class were denied privacy protections that they paid for and were entitled to receive, Plaintiff and the Class incurred actual monetary damages in that they overpaid for the products purchased from Target.[29]

Another alleges that plaintiffs sustained losses and damages because their personal and financial information was "exposed" and "compromised" as a result of the breach—with no specific claim of harm.[30] In the First Circuit, at least, such claims would probably fail on the same grounds as those in *Katz*: that the harm was "conjectural."[31]

One constant: each consumer's class action claims damages stemming from the expense of credit-monitoring. "Plaintiffs and the Class she seeks to represent now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights," states one complaint.[32] (This complaint and several others may be light on specifics because plaintiffs raced to file it on December 19, the same day Target acknowledged the breach and one day after a blogger first disclosed it.)

Target's decision to offer free credit-monitoring may foreclose claims by consumers that their paying for such services constituted "harm," to the extent courts even recognize injury in such an expense. The company first offered free credit monitoring services for "those impacted,"[33] then expanded it to cover "all guests" who shopped in Target's U.S. stores."[34]

Meanwhile, the U.S. Department of Justice, the U.S. Secret Service, and numerous state attorneys general are investigating, potentially leaving a rich trail for plaintiffs' lawyers.[35] Information reported about breaches to state attorneys general can become a matter of public record, providing grist for plaintiffs. Securities and Exchange Commission guidance now recommends that publicly traded companies disclose cyber-security risks and breaches.[36] It also suggests that companies involved in legal proceedings stemming from "a cyber incident" report the litigation in their disclosures.[37] Both types of disclosures seem sure to fuel shareholder derivative suits against officers and directors for depressed share prices following alleged failures to be sufficiently vigilant against cyber-attacks.[38]

The Target litigations will unfold for years to come, with outcomes we cannot foresee. What is clear is that plaintiffs' attorneys are already using the case to test creative new theories for establishing harm and obtaining standing. Target will ask courts to hold the line by maintaining their historic resistance to most such theories.

---

[1] *Anderson v. Hannaford Bros. Co.*, 659 F.3d 151, 167 (1st Cir. 2011) ("Plaintiffs' claims for identity theft insurance and replacement card fees involve actual financial losses from credit and debit card misuse. Under Maine contract law, these financial losses are recoverable as mitigation damages so long as they are reasonable.")

[2] *See* Raymond T. Nimmer, *Privacy & Personal Data Security: The Next Litigation Frontier?*, Washington Legal Found. (Jan. 16, 2009), http://www.wlf.org/upload/01-16-09Nimmer_LegalOpinionLetter.pdf.

ISBN 1056 3059

[3] *2013 Data Breach Investigations Report* at 11, Verizon, http://www.verizonenterprise.com/DBIR/2013/.
[4] *Attorney General Kamala D. Harris Releases Report on Data Breaches; 2.5 Million Californians Had Personal Information Compromised*, Cal. Dept. of Justice, Office of the Attorney Gen. (July 1, 2013), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-releases-report-data-breaches-25-million.
[5] *See* Ashley Post, *GCs Predict Increase in Consumer Fraud and Privacy Class Actions*, Inside Counsel (May 3, 2013), http://www.insidecounsel.com/2013/05/03/gcs-predict-increase-in-consumer-fraud-and-privacy.
[6] *See* Jason Weinstein, *Lessons From Recent Trends In Privacy Class Actions,* Law360 (Aug. 12, 2013), http://www.law360.com/privacy/articles/461229/lessons-from-recent-trends-in-privacy-class-actions.
[7] *See* Cory Andrews, *Encouraging Trend: Judges Can't "Stand" Online Privacy Class Actions*, The Legal Pulse, Washington Legal Found. (Jan. 24, 2013), http://wlflegalpulse.com/2013/01/24/encouraging-trend-judges-cant-stand-online-privacy-class-actions/.
[8] *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 120 S. Ct. 693, 704 (U.S. 2000).
[9] *See, e.g., Reilly v. Ceridian Corp.*, 664 F.3d 38, 43 (3d Cir. 2011) ("The present test is actuality, not hypothetical speculations concerning the possibility of future injury.").
[10] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1148 (2013).
[11] *See* Glenn Lammi, *Will California's New Data Breach Notification Duty Stimulate Class Action Litigation?*, The Legal Pulse, Washington Legal Found. (Oct. 3, 2013), http://wlflegalpulse.com/2013/10/03/will-californias-new-data-breach-notification-duty-stimulate-class-action-litigation/.
[12] Daniel J. Solove and Paul M. Schwartz, *Privacy Law Fundamentals 2013*, at 180-81 (Int'l Assoc. of Privacy Prof'ls. 2013). *See also Katz v. Pershing, LLC*, 672 F.3d 64, 79 (1st Cir. 2012) (plaintiff's purchase of credit-monitoring and insurance guard against "a purely theoretical possibility [that] simply does not rise to the level of a reasonably impending threat.")
[13] *Anderson*, 659 F.3d at 155-67.
[14] *Katz*, 672 F.3d at 79-80.
[15] *Id*. at 79.
[16] *Goodman v. HTC Am., Inc.*, No. 2:11-cv-01793-MJP, 2012 U.S. Dist. LEXIS 88496, at *19, (W.D. Wash. June 26, 2012).
[17] 18 U.S.C. § 2520.
[18] 18 U.S.C. § 2710.
[19] *Jewel v. NSA*, 673 F.3d 902, 908 (9th Cir. 2011) (quoting *Lujan v. Defenders of Wildlife*, 112 S. Ct. 2130, 2146 (1992).
[20] *Edwards v. First Am. Corp.*, 610 F.3d 514, 515-17 (9th Cir. 2010).
[21] 132 S. Ct. 2536 (2012).
[22] *See* David F. McDowell, D. Reed Freeman Jr., and Jacob M. Harper, *Privacy Class Actions: Current Trends and New Frontiers in 2013*, Bloomberg Law, http://about.bloomberglaw.com/practitioner-contributions/privacy-class-actions-current-trends-and-new-frontiers-in-2013/.
[23] *See* Eddie Makuch, *Xbox One Terms of Service Prevent Class-Action Suits*, Gamespot (June 12, 2013), http://www.gamespot.com/news/xbox-one-terms-of-service-prevent-class-action-suits-6410038.
[24] 131 S. Ct. 1740 (2011).
[25] One of the complaints was filed by a bank and purports to represent a class of financial institutions, not consumers. *See* Complaint, *Putnam Bank v. Target Corp.*, No. 0:14-cv-00121-DSD-JSM, Dkt. No. 1 (D. Minn. Jan. 13, 2014).
[26] Complaint ¶ 6, *Savedow v. Target Corp*., No. 0:13-cv-62790-WJZ, Dkt. No. 1 (S.D. Fla. Dec. 26, 2013).
[27] *Id*., ¶¶ 27-36.
[28] The authors recognize that nothing in Federal Rule of Civil Procedure Rule 8(a)(2), stating that a claim for relief contain only "a short and plain statement of the claim showing that the pleader is entitled to relief," requires a plaintiff to set forth in detail the alleged harm.
[29] Complaint ¶ 46, *McPherson v. Target Corp.*, No. 1:13-cv-09188, Dkt. No. 1 (N.D. Ill. Dec. 24, 2013).
[30] Complaint ¶ 21, *Rothschild v. Target Corp.*, No. 1:13-cv-00178-EJF, Dkt. No. 2 (D. Utah Dec. 23, 2013).
[31] *Katz*, 672 F.3d at 79-80.
[32] Complaint ¶ 25, *Wredberg v. Target Corp.*, No. 3:13-cv-5901, Dkt. No. 1 (N.D. Cal. Dec. 19, 2013).
[33] *See A Message from CEO Gregg Steinhafel about Target's Payment Card Issues*, (Dec. 20, 2013), http://pressroom.target.com/news/a-message-from-ceo-gregg-steinhafel-about-targets-payment-card-issues.
[34] *See Target Provides Update on Data Breach and Financial Performance*, (Jan. 10, 2014), http://pressroom.target.com/news/target-provides-update-on-data-breach-and-financial-performance.
[35] *See* Sara Germano and Robin Sidel, *Target Discusses Breach With State Attorneys*, The Wall Street Journal (Dec. 23, 2013), at http://online.wsj.com/news/articles/SB10001424052702304020704579276901918248632?KEYWORDS=target+and+%22attorneys+general%22; Kevin Johnson, *Feds Investigating Target Data Breach*, USA Today (Jan. 29, 2014), at http://www.usatoday.com/story/money/business/2014/01/29/target-data-breach-holder/5024739/.
[36] *Securities and Exchange Commission Division of Corporation Finance CF Disclosure Guidance: Topic No. 2*, *Cybersecurity* (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[37] *Id*.; Jason Weinstein, *supra.*
[38] *Id*.

  ISBN 1056 3059