10 August 2016

Practice Groups:

Financial Institutions and Services Litigation

Consumer Financial Services

Class Action Litigation Defense

Hold On, You Didn't Overpay for That: Courts Address New "Overpayment" Theory from Plaintiffs in Data Breach Cases

By Andrew C. Glass, David D. Christensen, and Matthew N. Lowe

With the ever-increasing amount of personal information stored online, it is unsurprising that data breach litigation has become increasingly common. A critical issue in nearly all data breach litigation is whether a plaintiff has standing to pursue claims—especially where there is no evidence of actual fraud or identity theft resulting from the purported data breach. The plaintiffs' bar has pursued a litany of legal theories in the attempt to clear the standing hurdle, including the recent theory of "overpayment" (a/k/a "benefit of the bargain" theory). Under this theory, the plaintiff alleges that the price for the purchased product or service—whether sneakers, restaurant meals, or health insurance—included some indeterminate amount allocated to data security. Depending on how the theory is framed, the purported "injury" is either that the plaintiff "overpaid" for the product or service, or that the plaintiff did not receive the "benefit of the bargain," because the defendant did not appropriately use the indeterminate amount to provide adequate data security. Despite plaintiffs' attempts to establish standing through this novel theory, courts have limited its applicability in a variety of ways discussed below.

Recent Article III Standing Development

Article III standing is a prerequisite to sustaining an action in federal court.[1] To establish standing, a plaintiff must have an injury that is "concrete, particularized, and actual or imminent," "fairly traceable to the challenged action," and "redressable by a favorable ruling."[2] In *Spokeo, Inc. v. Robins*,[3] the Supreme Court recently reemphasized that an injury must be both "concrete" *and* "particularized" to create standing.[4] The Supreme Court held that "concreteness" means the injury "actually exist[s]," and as applied to the facts of *Spokeo*, that "a bare procedural violation, divorced from any concrete harm" does not satisfy the injury-in-fact requirement of standing.[5]

Standing in Data Breach Cases

Standing is often hard to establish in the quintessential data breach case—where the plaintiff alleges that "hackers" breached the defendant's data system and absconded with personal information. Standing is even harder to establish where the plaintiff merely alleges that the defendant's data security is vulnerable, is easily compromised, or is not up to industry standards. In those circumstances, the plaintiffs' bar has pursued a variety of theories as to how the plaintiff has suffered an Article III injury—which courts have often rejected—including the increased risk of identity theft,[6] time spent monitoring or guarding against potential fraud,[7] and diminished value of plaintiffs' personal information.[8] Most recently, the plaintiffs' bar has asserted standing based on the overpayment theory discussed above. But

the theory is infirm and likely to be rejected by courts,[9] for the following reasons, among others:

First, where the plaintiff alleges only that the defendant's data security is vulnerable but was not actually breached, courts have held that the plaintiff lacks standing—including on an overpayment theory. Courts have reasoned that there can be no harm absent actual unauthorized access to a consumer's personal information, and even then additional evidence that injury occurred or is imminent may be necessary (i.e., evidence that the information accessed was used to commit fraud or will likely be misused).[10] Indeed, in the few cases where a court has found standing on an overpayment theory, the plaintiff's personal information was actually breached. And in most of these cases, the plaintiff alleged that her information was either accessed by unauthorized persons with nefarious intent or that the plaintiff also suffered actual identify theft as a result of the breach.[11] In short, mere speculation that the plaintiff's data *could have* or *may have* been disclosed to, or accessed by, a third party is insufficient to establish standing.[12]

Second, even where an actual data breach occurs, courts have analyzed the origins of the overpayment theory and rejected its application to the data breach context. The theory originated in products liability actions (i.e., that plaintiff overpaid for a product, because the product itself was defective).[13] The Seventh Circuit has stated that it is "dubious" that such a theory could be "extend[ed] … from a particular product to the operation of the entire store [where] plaintiffs allege that they would have shunned [the defendant business] had they known that it did not take the necessary precautions to secure their personal and financial data."[14] Another court rejected the overpayment theory in the data breach context because "[t]his is not the case where consumers paid for a product, and the product they received was different from the one as advertised on the product's packaging. Because Plaintiffs take issue with the way in which [the defendant] performed the security services, they must allege 'something more' than pure economic harm."[15]

Third, and closely related to the second point above, courts have rejected the overpayment theory in data breach cases where the payment was for a good or service unrelated to data security—e.g., shoes, food, health insurance, etc.—because the good or service itself was not defective.[16] Stated differently, a "[p]laintiff could not have 'overpaid' for the [good or] service he purchased because he received what he paid for" where there are no defects alleged in the good or service itself.[17] One court further explained that where the amount the plaintiff paid the defendant was for a membership and where the plaintiff received all of benefits of the membership, the plaintiff "merely alleging that [the defendant]'s privacy protections were not as stringent as she believed they would be" is insufficient to create standing.[18]

Fourth, courts have rejected the "creative" foundation of the overpayment theory—namely that a plaintiff can establish standing simply by alleging that some "indeterminate" amount paid for a good or service was for data security. In some cases, courts have required plaintiffs to be more specific in their pleadings about what portion was for data security.[19] As one court put it, "[t]o the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing."[20] In data breach cases targeting a specific payment method (e.g., credit cards), courts have rejected the overpayment theory for the additional reason that the plaintiff cannot allege that the price she paid for a product contained a portion for security to protect her

credit card information where a customer paying cash paid the same amount, yet needed no such security.[21]

Conclusion

The overpayment theory has not proved a panacea for the many standing problems that plaintiffs face in data breach cases. Yet, undoubtedly, the overpayment theory is not the last putative arrow in the plaintiffs' bar's quiver as they continue to pursue the hotbed of data breach litigation. And even if private data breach litigation is dismissed for lack of standing, there is still risk that a regulator may bring an enforcement action even absent an actual data breach, as the Consumer Financial Protection Bureau recently did.[22] At the same time, the Supreme Court's recent holding in *Spokeo*—that an injury must be concrete to establish standing; "that is, it must actually exist"[23]—will unquestionably affect standing questions in data breach litigation. K&L Gates will continue to monitor developments in data breach litigation and provide regular updates.

---

[1] *See*, *e.g.*, *Spokeo, Inc. v. Robins*, 578 U.S. ----, 136 S. Ct. 1540, 1547 (2016).

[2] *Clapper v. Amnesty Int'l USA*, 568 U.S. ----, 133 S. Ct. 1138, 1147 (2013) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010)); *see also Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-81 (2000).

[3] 578 U.S. ----, 136 S. Ct. 1540 (2016).

[4] *Id.* at 1548-49.

[5] *Id.*

[6] *See*, *e.g.*, *Chambliss v. Carefirst, Inc.,* 2016 WL 3055299, at *4 (D. Md. May 27, 2016) (rejecting increased risk of identity theft theory as "speculative" because it relies upon "a chain of assumptions that must occur before the harm materializes"); *Whalen v. Michael Stores Inc.*, 2015 WL 9462108, at *5 (E.D.N.Y. Dec. 28, 2015); *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 81792, at *4 (D. Minn. Jan. 7, 2016) ("In data security breach cases where plaintiffs' data has not been misused following the breach, the vast majority of courts have held that the risk of future identity theft or fraud is too speculative to constitute an injury in fact for purposes of Article III."); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 958-59 (D. Nev. 2015) ("increased threat of identity theft and fraud stemming from the Zappos's security breach does not constitute an injury-in-fact sufficient to confer standing"); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014).

[7] *See*, *e.g.*, *Chambliss,* 2016 WL 3055299, at *5 (paying for credit monitoring services alone could not create standing as this was nothing more than a "mitigation cost" that a plaintiff cannot expend to "manufacture standing"); *Whalen*, 2015 WL 9462108, at *3 (same); *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1087-88 (E.D. Cal. 2015); *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 81792, at *7 ("In data breach cases, courts consistently hold that the cost to mitigate the risk of future harm does not constitute an injury in fact unless the future harm being mitigated against is itself imminent."); *In re SAIC*, 45 F. Supp. 3d at 27 ("[Plaintiffs]' alleged time and money expenditures to monitor [] financial information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for [plaintiffs'] claims." (quoting *Reilly v. Ceridian Corp.*, 664 F.3d 38, 46 (3d Cir. 2011))).

[8] *See*, *e.g.*, *Whalen*, 2015 WL 9462108, at *4 ("[W]ithout allegations about how her cancelled credit card information lost value, Whalen does not have standing" on a loss of value to her personal identified information ("PII")); *In re SuperValu, Inc., Customer Data Sec. Breach Litig.*, 2016 WL 81792, at *7 (rejecting standing because "[p]laintiffs have not alleged that they tried to sell their PII but were not able to do so or were forced to accept a lower price"); *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 954 (same).

[9] *See*, *e.g.*, *In re Zappos.com, Inc. Cust. Data Sec. Breach Litig.*, 2016 WL 2637810, at *3-6 (D. Nev. May 6, 2016) (considering and rejecting numerous standing theories for plaintiffs that could not allege actual fraud or identity theft from data breach); *see also supra* n.6-8.

[10] *See*, *e.g.*, *Fernandez*, 127 F. Supp. 3d at 1088 (plaintiff lacked standing because he "has not alleged facts from which a plausible inference could be drawn that anyone viewed his PII/PHI as a result of the Data Breach"); *Katz v. Pershing, LLC*, 672 F.3d 64, 79-80 (1st Cir. 2012) (rejecting plaintiff's standing arguments, including her benefit of the bargain theory, because "plaintiff has not alleged that her nonpublic personal information actually has been accessed by any unauthorized person[, and] [h]er cause of action rests 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"); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013) (rejecting "overpayment" for security protocol theory where there was no allegation of "theft of their personally identifiable information"); *see also Khan v. Children's Nat'l Health Sys.*, 2016 WL 2946165, at *5 (D. Md. May 19, 2016) (even where there was a data breach, to show standing plaintiff must "put forth facts that provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud").

[11] *See Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1322 (11th Cir. 2012) (unsecured and unencrypted laptop computers containing plaintiffs' personal information were stolen by a third-party and "were sold to an individual with a history of dealing in stolen property"); *In re Anthem, Inc. Data Breach Litig.*, --- F. Supp. 3d ----, 2016 WL 589760, at *2 (N.D. Cal. Feb. 14, 2016) (security flaws "allowed cyberattackers to extract massive amounts of data from Anthem's database"); *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1206 (N.D. Cal. 2014) ("hackers" gained access to defendant's systems and "accessed the personal information of at least 38 million customers"); *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1105 (N.D. Cal. 2010) (defendant accidentally posted plaintiffs' personal information to the Internet where it was "downloaded and reposted on other websites").

[12] *See Strautins v. Trustwave Holdings, Inc.*, 27 F. Supp. 3d 871, 881 (N.D. Ill. 2014) (dismissing for lack of standing where plaintiff could only show that defendant was hacked but not that her data was among those actually accessed by the hackers).

[13] *See*, *e.g.*, *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 694 (7th Cir. 2015) (recognizing that overpayment theory typically arises in "cases involv[ing] products liability claims against defective or dangerous products").

[14] *Id.* at 694.

[15] *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013).

[16] *Chambliss,* 2016 WL 3055299, at *5-6; *Fernandez*, 127 F. Supp. 3d at 1089 (finding no standing where "[p]laintiff has not alleged facts from which a plausible inference could be drawn that he has been injured by a loss in value of his insurance coverage," which is the service he paid for); *In re SuperValu, Inc.*, 2016 WL 81792, at *8; *SAIC*, 45 F. Supp. 3d at 30; *Carlsen v. GameStop, Inc.*, 112 F. Supp. 3d 855, 862-63 (D. Minn. 2015) ("Plaintiff's consideration was for

enhanced content and he received the benefit of that bargain—the enhanced content. Therefore, security failures or misrepresentations relating to data security, even if true as alleged, cannot be a breach and thus cannot result in a breach-of-contract injury.").

[17] *Carlsen*, 112 F. Supp. 3d at 863; *see also Duqum v. Scottrade, Inc.*, 2016 WL 3683001, at *7 (E.D. Mo. July 12, 2016) (rejecting benefit of the bargain theory where plaintiffs did not "allege that the money they paid could have or would have bought a better policy with a more bullet-proof data-security regime"); *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968 (7th Cir. 2016) (rejecting application of overpayment theory to data breach claims because "such arguments have been adopted by courts only where the product itself was defective or dangerous and consumers claim they would not have bought it (or paid a premium for it) had they known of the defect").

[18] *Austin-Spearman v. AARP & AARP Servs. Inc.*, 119 F. Supp. 3d 1, 14 (D.D.C. 2015).

[19] *Chambliss,* 2016 WL 3055299, at *6 (finding no standing where plaintiffs "offer no factual allegations indicating that the prices they paid for health insurance included a sum to be used for data security"); *SAIC*, 45 F. Supp. 3d at 30; *Lewert v. P.F. Chang's China Bistro, Inc.*, 2014 WL 7005097, at *2 (N.D. Ill. Dec. 10, 2014) *reversed on other grounds by* 2016 WL 1459226 (7th Cir. Apr. 14, 2016) (dismissing for lack of standing where plaintiffs merely argued "the cost of the food they purchased *implicitly* contained the cost of sufficient protection of PII" (emphasis added)); *Carlsen*, 2015 WL 3538906, at *5 (finding no standing for data breach claim where "[p]laintiff does not allege that he paid anything specific for the Privacy Policy"); *see also Duqum*, 2016 WL 3683001, at *7 (finding plaintiffs did not have standing because "[a]lthough they allege in a conclusory fashion that a portion of the brokerage fees they paid to Defendant were for 'data management and security,' they do not allege any facts showing how any fee they paid was understood by both parties to be allocated toward the protection of customer data"). Unsurprisingly, courts have also rejected arguments that the defendant "passed on" an indeterminate amount of a payment to a third-party security vendor. *See Katz*, 672 F.3d at 77 (rejecting an argument "alleging that the fees [plaintiff] pays to [the payee] are higher than they otherwise would be because [the payee] 'passed on' the inflated charges for the defendant's service to her" because the "allegation is nothing more than a bare hypothesis that [the payee] possibly might push this aspect of its operational costs onto [the plaintiff]").

[20] *SAIC*, 45 F. Supp. 3d at 30.

[21] *See Whalen*, 2015 WL 9462108, at *3; *Lovell v. P.F. Chang's China Bistro, Inc.*, 2015 WL 4940371, at *6 (W.D. Wash. Mar. 27, 2015) (rejecting theory that plaintiff would have paid less for meal had he known restaurant's cybersecurity practices, because "customers pay the same price regardless of whether they pay with a credit card, debit card, check, or cash"); *In re Barnes & Noble Pin Pad Litig.*, 2013 WL 4759588, at *5 (N.D. Ill. Sept. 3, 2013) (rejecting allegation that plaintiffs "overpaid" for products and services purchased at retailer because the security measures were inadequate, "particularly as Plaintiffs have not pled that [the retailer] charged a higher price for goods whether a customer pays with credit, and therefore, that additional value is expected in the use of a credit card").

[22] *See* R. Bruce Allensworth, Ryan M. Tosi, Lindsay Sampson Bishop, *Proactive Protection of Consumers or Premature Penalty? Consumer Financial Protection Bureau Bucks the Trend in Data Security Breach Cases* (Mar. 15, 2016) *available at* www.klgates.com/proactive-protection-of-consumers-or-premature-penalty---consumer-financial-protection-bureau-bucks-the-trend-in-data-security-breach-cases/ (discussing CFPB's recent Consent Order with Dwolla, Inc.).

[23] *See*, *e.g.*, *Spokeo, Inc.*, 136 S. Ct. at 1548; *see also Khan*, 2016 WL 2946165, at *7 (dismissing data breach case for lack of standing and citing *Spokeo*).

Hold On, You Didn't Overpay for That: Courts Address New "Overpayment" Theory from Plaintiffs in Data Breach Cases

Authors:

Andrew C. Glass
andrew.glass@klgates.com
+1.617.261.3107

David D. Christensen
david.christensen@klgates.com
+1.617.951.9077

Matthew N. Lowe
matthew.lowe@klgates.com
+1.617.951.9183