Bloomberg BNA

Privacy and Security Law Report®

Standing

When actual injuries are claimed in a data breach case, overpayment allegations shouldn't be necessary to establish standing under Article III. However, where the injury-in-fact is based only on speculative future harm, adding an overpayment claim—added costs for information security supposedly passed onto consumers—likely won't be sufficient to carry the day, the author says.

Data Breaches

The Increasing Failure of 'Overpayment' Claims In Data Breach Litigation Against Retailers

BY JASON M. BEACH

Sufficient injury to establish Article III standing is a hotly contested—and sometimes dispositive—issue in data breach litigation.

Plaintiffs have been surviving Rule 12(b)(1) standing assaults with increasing frequency, and the Supreme Court of the United States' grant of certiorari in *Spokeo, Inc. v. Robins*, 135 S. Ct. 1892 (2015) (14 PVLR 779, 5/4/15), ultimately may help clarify some of the conflicting standing theories.

Currently, however, federal courts disagree on the types of injuries that satisfy standing for data breach plaintiffs. And one injury-in-fact theory has received less attention than many of the others: overpayment.

Overpayment theories are not new in areas such as products liability. They typically focus on misrepresentations, defects, or dangerous products. But overpayment in the data breach context generally goes one step further. Plaintiffs typically allege that information security costs are passed through to customers with higher prices on all products, and when information is breached, the consumer is injured by paying those allegedly inflated prices. Often, the overpayment claim is not based on any misrepresentation or product defect.

Is this application of the overpayment theory gaining traction with courts? Perhaps in some areas of privacy litigation, but not in data breach class actions. Indeed, a recent breach case decided by the Seventh Circuit criticized the overpayment theory as ''problematic,'' and was doubtful that it could independently establish standing. *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. July 20, 2015)(14 PVLR 1351, 7/27/15). This article examines the increasing failure of overpayment claims in federal data breach class actions against retailers.

Jason M. Beach is a counsel at Hunton & Williams, Atlanta. His practice focuses on complex commercial litigation, cybersecurity/data breach issues, and government regulatory matters. He often represents clients in high-profile class actions resulting from data exposures, and can be reached at jbeach@hunton.com.

 ISSN 1538-3423

Overpayment Claims in a Nutshell

Overpayment claims are not new, and typically involve manufacturer misrepresentations and/or products that are defective or dangerous. *See Remijas v. Neiman Marcus Grp.*, LLC, 794 F.3d 688 (7th Cir. July 20, 2015) (citing non-data breach overpayment cases). In the general privacy litigation context (excluding data breach cases, which are addressed in the sections below), overpayment claims have had mixed success. For example, *In re Google Android Consumer Privacy Litigation* involved the collection of personally identifiable information (PII) of consumers who purchased mobile phones with the Android operating system. 2013 BL 81669, No. 11-MD-02264 (N.D. Cal. Mar. 26, 2013) (unpublished) (12 PVLR 604, 4/8/13). One of the standing allegations was that the plaintiffs ''overpaid for their Android mobile devices.'' *Id.* The court recognized that overpaying for goods, or buying goods you otherwise would not have purchased, based on the seller's misrepresentations, can establish injury-in-fact sufficient for Article III standing. *Id.*

However, the court found insufficient facts to establish an injury based on overpayment. *Id.* The court explained that the plaintiffs had not alleged ''which Android devices they purchased or how much those devices cost. They also [did] not allege that had they known of the . . . [d]efendants' practices, they either would not have purchased an Android device or would not have paid what they did for such devices.'' *Id.* The plaintiffs also failed to ''identify what statements were material to their decision to purchase an Android device.'' *Id. But see In re Carrier IQ, Inc. Consumer Privacy Litig.*, 2015 BL 14643, No. C-12-MD-2330 EMC (N.D. Cal. Jan. 21, 2015) (denying motion to dismiss on overpayment claim associated with software embedded in mobile devices) (14 PVLR 157, 1/26/15); *Opperman v. Path, Inc.*, 2014 BL 134433, No. 13-CV-00453 (N.D. Cal. May 14, 2014) (finding sufficient injury-in-fact for standing based on overpayment claim) (13 PVLR 885, 5/19/14).

In data breach cases, overpayment allegations are fairly formulaic: customers overpaid for goods or services because the price included added costs for information security, and that protection was non-existent or inadequate, as evidenced by the data breach. *See, e.g.*, *Moyer v. Michaels Stores, Inc.*, 2014 BL 198944, No. 14-C-561 (N.D. Ill. July 14, 2014) (13 PVLR 1276, 7/21/14). Although data breach plaintiffs assert overpayment theories in various ways, they often are set forth as a measure of injury or are anchored to a substantive claim.

For example, a data breach complaint against The Home Depot articulated the overpayment theory in its unjust enrichment count. In these allegations, there were no facts suggesting that the products purchased were defective in any real sense, nor were there facts regarding a specific product representation. Rather, the allegations could be applied to any Home Depot product or service:

> The monies paid for the purchase of goods by Plaintiffs and members of the Class to Home Depot during the period of the Home Depot data breach were supposed to be used by Home Depot, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiffs and members of the Class.
>
> Home Depot failed to provide reasonable security, safeguards and protection to the personal and financial information of Plaintiffs and Class members and as a result, Plaintiffs and Class members overpaid Home Depot for the goods purchased through use of their credit and debit cards during the period of the Home Depot data breach.
>
> Home Depot should not be permitted to retain the money belonging to Plaintiffs and members of the Class, because Home Depot failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class members' personal and financial information that they paid for but did not receive.
>
> *Solak v. Home Depot*, No. 1:14-CV-02856-WSD, Compl. at ¶¶ 82-84 (N.D. Ga. Sept. 4, 2014).

In contrast to the mobile phone cases addressed above, the allegations in *The Home Depot* case (and many data breaches against retailers) involve the purchase of products that have no intrinsic characteristics associated with information security or privacy, or that relate to misrepresentations. Rather, the overpayment theories push the traditional concept past a specific product and onto an entire store. In this context, overpayment theories unravel. In fact, federal courts around the country overwhelmingly have rejected overpayment claims in data breach litigation against retailers.

Standing Concerns When Equal Prices Are Charged for Cash and Credit Purchases

Most overpayment analysis in data breach cases occurs in the Federal Rule of Civil Procedure 12(b)(1) context for lack of standing. For example, *In re Barnes & Noble Pin Pad Litigation* arose from unauthorized PIN-pad skimming used to hack customer information. 2013 BL 234605, No. 12-CV-8617 (N.D. Ill. Sept. 3, 2013) (12 PVLR 1541, 9/9/13).

The putative class action complaint advanced an overpayment theory to help establish injury. *Id.* Specifically, the plaintiffs alleged they overpaid for products and services because they paid, in part, for protective information security measures. *Id.* According to the plaintiffs, Barnes & Noble's alleged failure to employ those measures thus ''diminished the value'' of the products. *Id.* But, the court held that plaintiffs ''have not pled that Barnes & Noble 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.'' *Id.* The court thus concluded that ''this [overpayment] theory of damages is insufficient to establish standing.'' *Id.*

In *Lewert v. P.F. Chang's China Bistro, Inc.*, the court also rejected overpayment claims asserted by a putative class involving an estimated seven million credit and debit cards. 2014 BL 347354, No. 14-CV-1487 (N.D. Ill. Dec. 10, 2014) (13 PVLR 2162, 12/22/14). The *Lewert* plaintiffs contended the cost of the food they purchased at P.F. Chang's ''implicitly contained the cost of sufficient protection'' for the compromised data. *Id.* Because that data was hacked, they believed they had overpaid for their food and thus suffered a financial injury sufficient to confer standing. Citing the *Barnes & Noble* case, the *Lewert* court found that the lack of allegations of higher prices for card-paying customers was fatal to the overpayment claim. *Id. See also Green v. eBay Inc.*, 2015 BL 129558, No. 14-1688 (E.D. La. May 4, 2015) (dismissing overpayment claims for lack of standing when the plaintiff did not allege ''an injury-in-fact with respect to overpayment'').

  PVLR ISSN 1538-3423

Under these cases, overpayment claims in situations where cash- and card-paying customers pay equal prices may not establish Article III standing.

Standing Concerns When Value-Reducing Deficiency Is Extrinsic to Products Sold

The court in *Remijas v. Neiman Marcus Group, LLC*, set forth an additional standing-based reason to reject an overpayment claim in the data breach context. 2014 BL 256935 (N.D. Ill. Sept. 16, 2014) (13 PVLR 1646, 9/22/14), *rev'd on other grounds*, 794 F.3d 688 (7th Cir. July 20, 2015). *Remijas* was a putative class action that arose from hackers compromising hundreds of thousands of customers' payment card information and personally identifiable data. *Id.* Plaintiffs alleged they had paid a premium for retail goods, and the defendant was required to allocate a portion of that price to provide adequate information security. *Id.* Because the defendant suffered a data breach, the plaintiffs contended that they overpaid for their purchases. This overpayment, plaintiffs believed, was a financial injury sufficient to establish standing. *Id*.

Although the *Remijas* court credited the plaintiffs' overpayment theory for its creativity, it ultimately found it unpersuasive. *Id.* The court reasoned that the plaintiffs' authority stemmed from defective product cases (such as toxic children's toys), which found that financial loss—even in the absence of physical harm—can satisfy the requisite injury for standing purposes. *Id.* However, ''a vital limiting principle to this theory of injury is that the value-reducing deficiency is always *intrinsic* to the product at issue.'' *Id.* (emphasis added). The court explained that the alleged information security deficiency at issue was *extrinsic* to the retail goods at issue in *Remijas*. *Id.* The court illustrated the problem as follows:

> [S]uppose a retail store does not allocate a sufficient portion of its revenues to providing adequate in-store security. A customer who is assaulted in the parking lot after patronizing the store may well have a negligence claim against the store owner. But could he or she really argue that she overpaid for the products that she purchased? Or even more to the point: even if no physical injury actually befell the customer, under Plaintiffs' theory, the customer still suffered financial injury because he or she paid a premium for adequate store security, and the store security was not in fact adequate. *Id.*

Although the theory of injury appeared ''plainly sensible'' to the court, ''expanding it to include deficiencies extrinsic to the purchased product would effectively render [the theory] meaningless.'' *Id.*

The United States Court of Appeals for the Seventh Circuit subsequently reversed and remanded the trial court's decision dismissing the case. However, it is notable that the Seventh Circuit did not reverse the dismissal due to the trial court's overpayment analysis. Rather, the appellate court seemed to embrace the prior analysis. It characterized the overpayment theory as ''problematic,'' ''not necessary,'' and unlikely to establish standing by itself. *Remijas*, 794 F.3d 688. The Seventh Circuit also recognized that it and other courts have ''held that financial injury in the form of an overcharge can support Article III standing'' mostly in products liability cases involving defective products. *Id.* But, echoing the trial court's analysis, the appellate court refused to take the plaintiffs' invitation to extend those theories from ''a particular product to the operation of the entire store.'' *Id.* This reasoning opens the door for retailers to more effectively combat overpayment theories. It also signals to plaintiffs' attorneys that the most injury-in-fact traction arises from more concrete allegations of injury.

Claims May Be Implausible For Equal-Price Scenarios

While addressed mostly as a standing issue, an additional reason overpayment claims fail under Rule 12(b)(6) is due to a very basic pleading problem with unsupported inference and speculation. Outside the *retailer* data breach context, at least one federal circuit court has upheld the overpayment theory in a data breach. *Resnick v. AvMed, Inc.*, arose from data accessed from laptop computers stolen from a health plan provider. 693 F.3d 1317, 1322 (11th Cir. 2012) (11 PVLR 1413, 9/17/12). The *Resnick* plaintiffs alleged an overpayment theory grounded in unjust enrichment, which the trial court ultimately dismissed. The Eleventh Circuit, however, reversed, finding the following facts sufficient to withstand dismissal under Rule 12(b)(6):

- The plaintiffs allegedly had conferred a monetary benefit (monthly premiums) on the defendant.
- The defendant supposedly appreciated or had knowledge of the benefit.
- The defendant, according to the plaintiffs, used the premiums to pay for the administrative costs of data management and security.
- The defendant should not be permitted to retain the money belonging to the plaintiffs because the defendant allegedly failed to implement, or inadequately implemented, the data management and security measures that are mandated by industry standards, as evidenced by the data breach. *Id.* at 1328.[1]

The *Resnick* decision did not address the intrinsic versus extrinsic distinction that the later *Remijas* trial court decision found dispositive. However, the Seventh Circuit's subsequent and critical treatment of the overpayment theory distinguished *Resnick*. *Remijas*, 794 F.3d 688.

Moreover, *Resnick* has not translated into data-breach plaintiffs succeeding with overpayment claims against retailers. The court in *In re Target Corp. Customer Data Security Breach Litigation* explicitly disagreed with *Resnick*'s overpayment analysis under Rule 12(b)(6) due to implausibility. 66 F. Supp. 3d 1154 (D. Minn. Dec. 18, 2014) (14 PVLR 15, 1/5/15). Unlike *Resnick*, the *Target* case involved a retail data breach. The *Target* court reasoned:

> In [*Resnick*], every member of the health care plan paid the allegedly increased charge for data security because every member's personal information was at risk from insufficient security. But the same is not true at Target. Target charges all shoppers the same price for the goods they buy

[1] Circuit Judge William Pryor dissented from the *Resnick* majority's unjust enrichment analysis. He reasoned that Florida law prohibited a quasi-contractual claim (such as unjust enrichment) when an express contract governed the subject matter, which the parties did not dispute existed. 693 F.3d at 1332 (Pryor, J. dissenting).

> whether the customer pays with a credit card, debit card, or cash. But cash customers face no risk that a computer hacker will steal their personal information. If Target charged credit- and debit-card customers more for their purchases to offset the costs of data security, Plaintiffs might have a plausible allegation in this regard. *But the fact that all customers regardless of payment method pay the same price renders Plaintiffs' overcharge theory implausible. Id.* (emphasis added).[2]

Implausibility is a fatal defect under the pleading standards articulated by the Supreme Court of the United States in *Ashcroft v. Iqbal*, 556 U.S. 662, 677–80 (2009), and *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 554–63 (2007).

Retailers with brick-and-mortar stores where customers can pay with cash may be better able to avoid *Resnick*'s reach and take advantage of cases that employ reasoning similar to the *Target* case. In other words, *Target*'s 12(b)(6) overpayment analysis also aligns with *Lewert*'s 12(b)(1) focus on equal prices for cash- and card-paying customers. *Lewert*, 2014 BL 347354. In the 12(b)(6) context, equal prices suggest the implausibility of customers' alleged expectations for additional value when paying with credit and debit cards, and thus may be more susceptible to dismissal.

Can Claims Survive Dismissal With More Particularized Pass-Through Allegations?

Would alleging additional facts about the allocation or pass-through of higher prices save data breach overpayment claims from dismissal? In most cases, perhaps not. On the one hand, retailers are making more disclosures how they protect PII, often in their online privacy policies, including how they protect customer's PII associated with debit and credit card purchases. For example, Target's privacy policy states:

> We maintain administrative, technical and physical safeguards to protect your personal information. When we collect or transmit sensitive information such as a credit or debit card number, we use industry standard methods to protect that information. However, no e-commerce solution, website, database or system is completely secure or ''hacker proof.'' You are also responsible for taking reasonable steps to protect your personal information against unauthorized disclosure or misuse. http://www.target.com/spot/privacy-policy#InfoProtect (last visited August 7, 2015).

However, retailers generally do not disclose to customers how these safeguards affect product pricing, if at all. Plaintiffs therefore may argue, as did the *Remijas* plaintiffs, that ''[t]he costs incurred by any retailer for implementation of security measures are passed along to *all* consumers in the form of higher prices for products.'' *Remijas v. Neiman Marcus Group, LLC*, No. 14-3122, Br. of Pls., Doc. 12 at 21 (7th Cir. Nov. 5, 2014) (available via CM/ECF or PACER). Citing a *USA Today* article, the *Remijas* plaintiffs also extended the same argument to costs resulting from data breaches. *Id.* n.6. Accordingly, the *Remijas* plaintiffs contended, those allegations must be accepted as true on their face. *Id.*

On the other hand, several problems remain. As noted in the *Target* case, most retailers charge all their customers the same prices, regardless of whether they pay with cash or a debit/credit card, despite the fact that cash customers are not at risk of their financial information being stolen. However, retailers who charge customers who pay with cash different prices than those who pay with debit/credit cards may be in a different position. Additionally, the extrinsic versus intrinsic distinction articulated by the *Remijas* trial court—and later endorsed in dicta by the Seventh Circuit—nevertheless exists for the products sold by many retailers. Thus, problems may remain with both the Federal Rule of Civil Procedure 12(b)(1) (insufficiency to establish standing) and 12(b)(6) (implausibility regarding the ability to state a claim).

Conclusion

At its base, the overpayment theory in data breach cases rests on general economic speculation that information security costs are passed along to consumers in the form of higher prices. This is the point where the real persuasion will shape the jurisprudence.

Is the issue merely one of pleading facts—within the bounds of Federal Rule of Civil Procedure 11—that a court should accept as true at the Rule 12 stage, only to be tested by the evidence at a later point? Or, does such economic speculation and financial conjecture fail to meet the *Twombly* and *Iqbal* thresholds for pleading?

In a non-retail data breach case, the United States Court of Appeals for the First Circuit held that ''the plaintiff's [overpayment] allegation is nothing more than a bare hypothesis that [a defendant] might push this aspect of its operational costs onto her. This is not a plausible allegation that the false advertisements [that it adequately protects customer data] caused her to pay the supposedly inflated prices.'' *Katz v. Pershing, LLC*, 672 F.3d 64, 77 (1st Cir. 2012) (affirming dismissal of data breach claims due to lack of standing) (citing *Iqbal* and *Twombly*) (11 PVLR 421, 3/5/12).

The answer largely will depend on the facts. In cases where sufficiently actual and concrete injuries have been alleged in a data breach case, overpayment should not be necessary to establish standing under Article III. *Remijas*, 794 F.3d 688.

However, where the injury-in-fact is based only on speculative future harm (to which courts have not been receptive), adding an overpayment claim likely will not be sufficient to carry the day. *See id.* (doubting whether overpayment theory could establish standing independently). Additionally, jurisdictions such as the Eleventh Circuit may be more receptive than courts in the Seventh or First Circuits. Finally, even if plaintiffs hurdle the initial standing bar, they may not make it past a Rule 12(b)(6) motion.

[2] Another court, having found at least one injury to support standing, declined to engage the overpayment issue in its standing analysis. *Moyer v. Michaels Stores, Inc.*, 2014 BL 198944 (N.D. Ill. July 14, 2014). The court nevertheless rejected the overpayment theory for failure to state a claim (under Fed. R. Civ. P. 12(b)(6)). *Id.* Without much explanation, the *Moyer* court found that the plaintiffs failed to have ''pled enough facts to support an inference that Michaels charged customers a premium for data security protection.'' *Id.*