Bloomberg Law

Privacy and Security Law Report®

Breach Litigation

Data-breach plaintiffs are looking for new avenues into the courtroom, such as using ''overpayment'' theory in an attempt to demonstrate that they have suffered injury sufficient to give them standing to sue, the author writes, discussing what companies should know about these new theories.

Litigation

Defending Novel Theories of Harm in Data-Breach Litigation

By Alex Pearce

The success of a data-breach lawsuit often turns on whether the plaintiff has standing to sue. Showing actual injury can be especially hard when the only alleged damage consists of a risk of future identity theft.

Data-breach plaintiffs are therefore looking for new avenues into the courtroom. One of these avenues is an ''overpayment'' theory.

This theory rests on the premise that the price of a product or service includes a payment for measures to protect the buyer's personal information. When a data breach compromises that information, the buyer alleges that he or she has overpaid for the product or service because the seller failed to provide the agreed-upon measures.

Alex Pearce is a privacy and data security attorney at Ellis & Winters LLP in Raleigh, N.C.

In two recent federal court decisions, data-breach plaintiffs successfully used overpayment theories to clear the Article III standing hurdle. But in each, the claims were nonetheless dismissed under Federal Rule 12(b)(6).

Taken together, these decisions contain some important lessons for businesses seeking to stifle data-breach lawsuits that are premised on this increasingly popular theory of injury.

A Toy Story *In In re VTech Data Breach Litigation*, No. 15-CV-10889 (N.D. Ill. Jul. 5, 2017) VTech Electronics North America LLC sold learning toys for young children. These toys, which included tablet computers and other handheld electronics, connected to VTech's online application store, from which customers could purchase and download games, books, music, and videos. Some toys could also connect to an online service that enabled children to exchange text, picture, and voice messages with their parents' cellphones.

To access these services, customers had to register for online accounts with VTech. Parents who registered provided personal information about themselves and their children to VTech. Parents also had to agree to terms and conditions that incorporated VTech's privacy policy. In that policy, VTech promised to protect personal information through certain data-security measures.

In 2015, a hacker infiltrated VTech's servers and downloaded the personal information of over ten million adults and children. The plaintiffs—purchasers of VTech's toys who had also registered for the online services—sued VTech and alleged that the hack resulted from VTech's failure to live up to its data secu-

 ISSN 1538-3423

rity promises. Their complaint asserted various claims, including one for breach of contract.

The plaintiffs alleged that their injuries consisted of an economic harm: receiving a product worth less than the one for which they paid. According to the plaintiffs, the ''product'' they paid for included the toys, the online service, and the promised data-security measures.

You Only Get What You Pay For VTech rejected that characterization of the transaction and moved to dismiss for lack of standing and for failure to state a claim.

According to VTech, buyers participated in two transactions:

1. a purchase transaction involving the plaintiffs' payment for a standalone physical toy, and
2. the plaintiffs' registration for the online services, an optional but separate—and free—offering.

Because VTech had only made data-security promises in the second transaction, VTech argued that the plaintiffs could not establish any ''overpayment'' for the physical toys that would constitute an injury-in-fact for Article III purposes.

For the same reason, VTech argued, the plaintiffs could not establish a key element of their breach of contract claim, namely, that both parties understood and intended that a portion of the purchase price for the toys would be allocated to protecting personal information collected through the online service.

Overpayment for Data Security Can Be an Injury-in-Fact The court denied VTech's arguments as to standing.

The court observed that economic injury can result ''from being given a different, less valuable product than the one that was promised and paid for,'' and that such an injury meets Article III's injury-in-fact requirement. By alleging such an injury—one consisting of overpayment for VTech's toys and the associated online services—the plaintiffs had satisfied Article III's injury-in-fact requirement.

The court also noted, however, that whether an injury-in-fact had been sufficiently alleged was separate and distinct from whether the complaint plausibly stated a claim that would entitle the plaintiffs to recover damages.

But the Plaintiffs Didn't Pay for Data Security Turning to that question, the court acknowledged the parties' disagreement as to what the purchase contract included, but held that VTech had the better of that argument. To that end, it agreed with VTech that ''there is a difference between selling a product that combines both a physical toy and a service, and selling a physical toy whose features may be supplemented by a separate service that VTech provided for free.''

The court then concluded that VTech had done the latter. To support that conclusion, the court observed that the toys functioned without the online services. In addition, the online-services terms did not suggest that the plaintiffs ''purchased'' the online services, or that the parties intended to incorporate those terms into the purchase contract for the toys.

The court thus held that the plaintiffs had failed to show that both parties understood a portion of the purchase price for the toys would be allocated to the protection of personal information submitted through the online services.

The court concluded this failure was fatal to the plaintiffs' breach of contract claim, and granted VTech's motion to dismiss.

Getting Off Scott-Free? *Kuhns v. Scottrade, Inc.*, Nos. 16-3426, 16-3542 (8th Cir. Aug. 21, 2017) involved a more straightforward data-breach scenario. There, hackers accessed the internal customer database of Scottrade Inc., a securities brokerage firm. The hackers acquired sensitive personal information of over 4.6 million customers. They then used that personal information to operate a stock price manipulation scheme, illegal gambling websites, and a bitcoin exchange.

The plaintiffs—Scottrade customers whose personal information was accessed by the hackers—sued Scottrade in federal court in Missouri. Their complaint asserted claims for breach of express and implied contract.

According to the plaintiffs, a portion of the fees they paid to Scottrade for brokerage services was to be used for data management and security. To that end, the plaintiffs pointed to representations that Scottrade made as part of their brokerage agreements.

That agreement included a ''Privacy and Security Statement'' in which Scottrade represented that it would:

- ''maintain physical, electronic and procedural safeguards that comply with federal regulations to guard your nonpublic personal information;'' and
- ''offer[ ] a secure server and password-protected environment . . . protected by Secure Socket Layer (SSL) encryption.''

The plaintiffs alleged that the hack occurred because Scottrade didn't live up to these promises.

For damages, the plaintiffs sought ''the monetary difference between the amount paid for services as promised . . . and the services actually provided.''

The district court dismissed the complaint for lack of standing. It concluded that the plaintiffs' ''conclusory'' allegations that they been deprived of the benefit of data management and security services that they paid for did not constitute a sufficiently concrete injury.

Overpayment = Concrete Injury On appeal, the U.S. Court of Appeals for the Eighth Circuit rejected that analysis. The Eighth Circuit pointed to its earlier decision in *Carlsen v. GameStop, Inc.*, No. 15-2453 (8th Cir. Aug. 16, 2016), which also involved claims premised on an overpayment theory. In that case, the court held that ''a party to a breached contract has a judicially cognizable interest for standing purposes, regardless of the merits of the breach alleged.''

The *Scottrade* plaintiffs satisfied that test. Their complaint alleged that they bargained for and expected protection of their personal information, and suffered a diminished value of that bargain when Scottrade failed to prevent the data breach. Thus, the Eighth Circuit concluded, the plaintiffs had standing to assert the breach of contract claims, ''whatever the merits'' might be of those claims.

Show Me the Breach As to the merits, Scottrade argued that even if the plaintiffs had standing, their contract claims that relied on the overpayment theory should still be dismissed under Rule 12(b)(6).

Scottrade argued that the plaintiffs did not allege any specific facts to establish that Scottrade breached its promises regarding data security. To that end, Scot-

  PVLR ISSN 1538-3423

trade observed, the plaintiffs hadn't alleged any specific security measures that Scottrade had promised but failed to implement. Nor had they specified any particular laws with which Scottrade's data security practices failed to comply.

Data Breach ≠ Contract Breach (Necessarily) The Eighth Circuit agreed with Scottrade.

It concluded that the plaintiffs had failed to allege any specific breach of the security representations in the brokerage agreement. To that end, the court observed that:

- the plaintiffs did not identify any specific law or regulation that Scottrade's data security practices violated; and
- Scottrade never affirmatively promised that its customers' data would not be hacked.

Acknowledging that the complaint presented the ''possibility'' of misconduct, the court nonetheless held that more was required: ''It is possible that Scottrade breached the Brokerage Agreement, but we have no idea how.''

Critically, the court concluded that the mere fact that data breach occurred could not supply the requisite factual basis for the breach of contract claims. It explained that ''the implied premise that because data was hacked Scottrade's protections must have been inadequate'' amounted to a ''naked assertion devoid of further factual enhancement'' that could not survive a motion to dismiss under the Supreme Court's ruling in *Ashcroft v. Iqbal*.

The court thus affirmed the district court's dismissal of the action, albeit under Rule 12(b)(6) rather than Rule 12(b)(1).

Implications for Companies *VTech* and *Scottrade* contain some important lessons for companies.

First, the specific language that a company uses in its privacy and data security representations to customers—and the context in which those representations are made—matters. Companies should avoid making unnecessary privacy and data security representations in customer agreements and terms of use. And when such representations need to be made, they should be presented in terms that avoid guarantees against security breaches, or that otherwise suggest a breach can't or won't occur.

Second, insofar as plaintiffs need to allege specifically how a company's security practices fell short to make out an overpayment claim, knowledge is power—especially when it comes to the facts and circumstances of a data breach. Companies should keep their internal breach investigations confidential, and avoid unnecessary public disclosures of details concerning the breach that prospective plaintiffs might use to craft an overpayment theory.

Finally, these decisions confirm that overpayment theories can provide a ready means for plaintiffs to defeat standing-based challenges, where other theories have consistently failed. But they also confirm that overpayment theories still face an uphill battle under Rule 12(b)(6). Smart defendants will demand that plaintiffs allege specific facts not only about the data security promises for which they paid, but also about the specific ways in which a defendant's practices failed to live up to those promises. As *Scottrade* makes clear, neither conclusory allegations of broken security promises, nor the mere fact of a data breach, should be sufficient to satisfy that burden.

BY ALEX PEARCE

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com