2009 WL 4798148
Only the Westlaw citation is currently available.
NOT FOR PUBLICATION
United States District Court,
D. New Jersey.

In re HEARTLAND PAYMENT SYSTEMS, INC. SECURITIES LITIGATION.

Civ. No. 09–1043.
|
Dec. 7, 2009.

West KeySummary

**1** **Securities Regulation**
Matters to Be Disclosed

Shareholders failed to state a claim under the Private Securities Litigation Reform Act (PSLRA) that a corporation misrepresented the state of its computer network security. Executives did not fail to disclose a structured query language (SQL) attack during an earnings conference call. In stating that there was no security incident that prompted certain security expenditures during the fourth quarter of that year, the executives were being truthful because the SQL attack occurred at the end of the year, after the expenditure had been made. Securities Exchange Act of 1934, § 21D(b)(2), 15 U.S.C.A. § 78u–4(b)(2).

Cases that cite this headnote

**Attorneys and Law Firms**

Douglas Wilens, Paul Jeffrey Geller, Coughlin Stoia Geller Rudman & Robbins LLP, Sabrina E. Tirabassi, Boca Raton, FL, Emily C. Komlossy, Jamie R. Mogil, Faruqi & Faruqi, New York, NY, Peter S. Pearlman, Cohn, Lifland, Pearlman, Herrmann & Knopf, LLP, Saddle Brook, NJ, Olimpio Lee Squitieri, Squitieri & Fearon, LLP, Jersey City, NJ, Daniel S. Sommers, Cohen, Milstein, Sellers & Toll, PLLC, Washington, DC, for Plaintiff.

David C. Kistler, Stephen M. Orlofsky, Blank Rome, LLP, Princeton, NJ, Seth J. Lapidow, Blank Rome, LLP, Cherry Hill, NJ, for Defendant.

OPINION

THOMPSON, District Judge.

*INTRODUCTION*

***1** This matter comes before the Court upon Defendants' Motion to Dismiss [20]. The Court has decided the motion upon the parties' written submissions and without oral argument. For the reasons given below, the motion is GRANTED.

*BACKGROUND*

For purposes of deciding this motion, the Court accepts the following allegations, which are set out in the Complaint, as true.

Heartland Payment Systems, Inc. ("Heartland") provides bank card payment processing services to merchants in the United States. (Compl. at ¶ 18.) The company facilitates the exchange of information and funds between merchants that accept credit and debit card payments and the cardholders' financial institutions. (*Id.*) In the course of administering these services, Heartland maintains millions of credit and debit card numbers on its computer network.

In December 2007, a group of hackers now under criminal indictment launched a "Structured Query Language" Attack[1] ("SQL attack") on Heartland's computer network, specifically the company's payroll manager application. (*Id.* at ¶¶ 5, 74.) The payroll manager application does not contain data on cardholders' credit and debit card accounts; rather, it contains internal corporate information such as employees' names, addresses, social security numbers, and other confidential

  

information. (*Id.* at ¶ 76.) Technology personnel at Heartland spent much of January "putting out fires" related to the attack, but no information was ever stolen off of the payroll manager. (*Id.* at ¶ 76.)

Unfortunately, while the SQL attack targeted the payroll manager application, the damage was not confined to this part of Heartland's computer network. The SQL attack resulted in hidden, malicious software being placed on Heartland's network. This malware ended up infecting not just the payroll manager application, but also the payment processing system, which was responsible for storing credit card data and debit card data. (*See id.* at ¶ 5.) Over the course of 2008, the hackers managed to steal 130 million credit card and debit card numbers. (*Id.*)

Heartland did not discover the breach until January 12 or 13, 2009. (*Id.* at ¶ 109.) The company immediately notified the U.S. Department of Justice, the U.S. Secret Service, and the credit card companies whose account numbers had been stolen. (*Id.*) Then, on January 20th, Heartland publicly disclosed the theft. (*Id.* at ¶¶ 108–09.) Following this disclosure and subsequent disclosures about the possible impact that the thefts might have on Heartland's business, Heartland's stock price dropped from more than $15 per share on January 19 to $5.34 per share by February 24. (*Id.* at ¶¶ 110–115.) If measured from its highest price during 2008, Heartland's stock suffered a total decline in value of almost 80%. (*Id.* at ¶ 133.) Plaintiffs, who purchased stock during 2008, suffered significant losses as a result of this decline in value.

***2** The alleged fraudulent acts took place in 2008, after Heartland had suffered the SQL attack but before it discovered the credit and debit card number thefts in January 2009. Plaintiffs claim that Heartland misrepresented the state of its computer network security through statements that Defendants Carr and Baldwin made on earnings conference calls and statements made in its 2007 Form 10–K report, which was filed with the Securities and Exchange Commission ("S.E.C .") in March of 2008. (*Id.* at ¶¶ 91–107.) Specifically, Plaintiffs contend that when asked about security incidents that occurred in 2007, Defendants concealed the SQL attack. (*Id.*) They also contend that Defendants made statements to the effect that Heartland had adequate security systems and that Heartland took the issue of computer network security very seriously. (*Id.*) Plaintiffs argue that these statements concerning the general state of security at Heartland are fraudulent because Carr and Baldwin were aware that Heartland had poor data security and had not remedied the problem. (*Id.*)

*ANALYSIS*

I. *Standard of Review*

Private securities fraud actions brought as class action lawsuits are subject to heightened pleading standards under the Private Securities Litigation Reform Act of 1995 ("PSLRA"). 15 U.S.C. § 78u–4(b). In cases governed by the PSLRA, "the complaint shall specify each statement alleged to have been misleading, the reason or reasons why the statement is misleading, and, if an allegation regarding the statement or omission is made on information and belief, the complaint shall state with particularity all facts on which that belief is formed." 15 U.S.C. § 78u–4(b)(1). These requirements are substantially similar to the heightened pleading standards under Fed.R.Civ.P. 9(b), requiring the plaintiff to plead the "who, what, when, where, and how" of the allegedly fraudulent statements. *Institutional Investors Group v. Avaya Inc.,* 564 F.3d 242, 252 (3d Cir.2009).

The PLSRA also requires that the complaint "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind." 15 U.S.C. § 78u–4(b)(2). The complaint will meet this standard only if the facts alleged support an inference of scienter that is "cogent and at least as compelling as any opposing inference of nonfraudulent intent." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.,* 551 U.S. 308, 314, 127 S.Ct. 2499, 168 L.Ed.2d 179 (2007). As the Supreme Court has explained, this is an "inherently comparative" analysis, requiring courts to "consider plausible nonculpable explanations for the defendant's conduct, as well as inferences favoring the plaintiff." *Id.* at 324. In other words, "the reviewing court must ask: When the allegations are accepted as true and taken collectively, would a reasonable person deem the inference of scienter at least as strong as any opposing inference?" *Id.* at 325. If the complaint does not satisfy these pleading requirements, the case must be dismissed. 15 U.S.C. § 78u–4(b)(3)(A).

***3** Only the misrepresentation and scienter elements of a private securities law claim are subject to heightened pleading standards under the PSLRA; the other elements of the claim are governed by the general pleading standards set out in Fed.R.Civ.P. 8(a). *Dura Pharmaceutials Inc. v. Broudo,* 544 U.S. 336, 346, 125 S.Ct. 1627, 161 L.Ed.2d 577 (2005). A court determining whether a complaint meets the requirements of Rule 8(a) must undertake the following two-step analysis:

  

> First, the factual and legal elements of a claim should be separated. The District Court must accept all of the complaint's well-pleaded facts as true, but may disregard any legal conclusions. Second, a District Court must then determine whether the facts alleged in the complaint are sufficient to show that the plaintiff has a "plausible claim for relief."

*Fowler v. UPMC Shadyside,* 578 F.3d 203, 210–11 (3d Cir.2009) (citing *Ashcroft v. Iqbal,* —— U.S. ——, —— – ——, 129 S.Ct. 1937, 1949–50, 173 L.Ed.2d 868 (2009)). For purposes of resolving a motion to dismiss, "plausible" does not mean "probable," but it requires more than "sheer possibility." *Iqbal,* 129 S.Ct. at 1949; *see also Bell Atlantic Corp. v. Twombly,* 550 U.S. 544, 556, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007). In other words, if the factual allegations are more likely explained by lawful behavior than illegal activity, then the complaint should be dismissed. *Iqbal,* 129 S.Ct. at 1950.

A claim for securities fraud requires the Plaintiff to prove six elements: (1) a material misrepresentation or omission, (2) scienter, (3) a connection with the purchase or sale of a security, (4) reliance, (5) economic loss, and (6) loss causation. *Dura Pharmaceuticals,* 544 U.S. at 341–42. Defendants attack the sufficiency of only three of these elements: misrepresentation, scienter, and loss causation.

II. *A Material Misrepresentation or Omission*

Plaintiffs' allegations of fraud fall into two general categories: allegations that Defendants fraudulently concealed the 2007 SQL attack and allegations that Defendants fraudulently misrepresented the general state of data security at Heartland. This Court's analysis will track the chronology of the allegedly fraudulent acts, first determining whether Plaintiff's failure to disclose the SQL attack in a specific February 2008 conference call was fraudulent, then analyzing whether any of Defendants' affirmative representations later on in 2008 were false, and finally discussing whether any of these affirmative representations—even if not literally false—nonetheless created a duty to disclose the SQL attack.

A. *Defendants' Failure to Disclose the 2007 SQL Attack During the February 2008 Earnings Conference Call*

On February 13, 2008, Defendants Carr and Baldwin participated in an earnings conference call with several financial analysts to discuss Heartland's fourth quarter 2007 financial results. Plaintiffs allege that Carr's and Baldwin's statements concealed the 2007 SQL attacks and related security problems. (Compl.¶¶ 91–94.) During the conference call, Carr and Baldwin discussed certain information technology and security expenditures that Heartland made during the last quarter of 2007. These general remarks prompted a couple analysts to ask whether there was any specific security incident that prompted Heartland to make those expenditures, to which Defendants basically answered, "No." Plaintiffs allege that this was untruthful because it conceals the fact that Heartland suffered the SQL attack.

***4** However, careful attention to context demonstrates that Defendants' statements and omissions on this conference call are not fraudulent.[2] The analysts' questions concerned certain expenditures that Heartland made during the fourth quarter of 2007. Obviously, any incident that prompted those expenditures would have occurred before the expenditures were made. The SQL attack occurred on December 26, far too late in the quarter to have been the cause for the million-plus dollar expenditure that was the subject of the analysts' questions. If the analysts had simply asked "Did you suffer a security lapse in fourth quarter 2007?" then Defendants' answers might very well have been misleading. But the analyst was specifically asking whether Heartland suffered a security incident *that caused the large fourth quarter IT expenditure.* Since the SQL attack did not cause the fourth quarter security expenditure, Defendants answered truthfully when they answered in the negative.

Plaintiffs allege that Defendant Baldwin made one other misrepresentation on the February 13 conference call—the following statement:

> With IT security you're either pregnant or you're not. And I think it would be irresponsible for us to know that we have vulnerabilities in our system where we could have something really bad happen that would put the Company in a TJ Maxx position. Now fortunately we've never had anything close to that happen but we could see a scenario where that could have happened. We don't see that anymore.

(Compl.¶ 93.) Plaintiff argues that this statement is untrue because Heartland had in fact suffered a significant security breach—the SQL Attack. However, this Court does not read the above paragraph as concealing that fact. A "TJ Maxx position" presumably refers to an incident in 2005 when hackers breached the T.J. Maxx Corporation's computer network and gained information on 45 million credit and debit card accounts. *See* "TJX Says Theft of Credit Card Data Involved 45.7 Million Cards," *New York Times,* March 30, 2007, at C2. As of February 2008, hackers had not stolen any credit card information from Heartland. So at the time the above statement was made, Heartland had not suffered the sort of security problem to which Baldwin was alluding. In other words, in the above-quoted passage, Baldwin was talking about security breaches that resulted in major financial problems. There are no allegations to the effect that, as of February 2008, Heartland had suffered any major headline-making problems of the sort T.J. Maxx experienced in 2005. Furthermore, Baldwin did not categorically assert that Heartland had never suffered any security problems; he merely stated that Heartland had not suffered anything "close to" what T.J. Maxx had suffered. His statement was therefore truthful.

B. *Affirmative Statements Concerning the General State of Data Security at Heartland*

1. *The 2007 Annual Report (S.E.C. Form 10–K) Filed on March 10, 2008*

***5** Heartland filed its annual report for the year 2007 with the S.E.C. on March 10, 2008. In one part, the report discussed Heartland's network security situation. The report stated that Heartland "place[d] significant emphasis on maintaining a high level of security" and maintained a network configuration that "provides multiple layers of security to isolate our databases from unauthorized access." (Compl.¶ 95.) The report also warned that Heartland's "computer systems could be penetrated by hackers" and that "[i]f the Company's network security is breached or sensitive merchant or cardholder data is misappropriated, the Company could be exposed to assessments, fines or litigation costs." (*Id.*) Plaintiffs argue that these statements are untruthful because Heartland had suffered the SQL attack and had not fully resolved security issues arising out of that attack. (*Id.* at ¶ 96.) However, there is nothing inconsistent between Defendants' statements and the fact that Heartland had suffered an SQL attack. The fact that a company has suffered a security breach does not demonstrate that the company did not "place significant emphasis on maintaining a high level of security." It is equally plausible that Heartland did place a high emphasis on security but that the Company's security systems were nonetheless overcome. In fact, given all the money that Heartland spent on security in late 2007 and the fact that Heartland did take steps to fix its security after the SQL breach (*id.* at ¶ 79), the latter explanation seems much more plausible. Since the alleged facts are more plausibly explained by lawful behavior than illegal deception, the claim does not satisfy Rule 8(a), let alone the PSLRA. *Iqbal,* 129 S.Ct. at 1949. The fact that there may have been unresolved security issues remaining in the wake of the 2007 attack does not contradict the 10–K either. Once again, the fact that a company faces certain security problems does not of itself suggest that the company does not value data security.

Plaintiffs attempt to bolster their allegations by relying on information provided by their confidential witness, a former Senior Developer at Heartland. Plaintiffs admit that "Heartland seemed focused on educating its developers about SQL Injection Attacks and figuring out a way to make those attacks less likely in the future" but argue that not enough was done to contain the breach that had already occurred. (Compl.¶ 79.) The former Senior Developer opines that "the Company should have built a new server with a clean copy of the operating system." (*Id.*) The former Senior Developer also complained of a variety of other practices at Heartland—unrelated to the 2007 breach or the 2008 data theft—that he felt put Heartland's data security at risk. (*Id.* at ¶¶ 45–65.) However, one former employee's opinion that Heartland did not do everything it could have done to address the security breach does not render the statement "We place significant emphasis on maintaining a high level of security" false. Furthermore, the cautionary statements in the Form 10–K—warning of the possibility of a breach and the consequences of such a breach—make clear that Heartland was not claiming that its security system was invulnerable.

***6** The facts alleged in the complaint do not support an inference that Heartland did not make serious efforts to protect its computer network from security breaches. Furthermore, the 10–K did not make any statements to the effect that the company's network was immune from security breaches or that no security breach had ever occurred. Therefore, the statements in the 10–K were not false or misleading.

2. *The November 4, 2008 Conference Call*

On November 4, 2008, Heartland held another conference call with analysts, this time to discuss third quarter 2008 financial results. On that call, Defendant Carr spoke about Heartland's need to adopt more secure technology for

  

processing transactions. (*Id.* at ¶ 106.) These statements were a mix of general observations concerning trends in encryption standards as well as indications that Heartland was going to adopt new technology being developed by American Express. (*Id.*) There is nothing in the Complaint that suggests that these forward-looking statements turned out to be false. They have nothing to do with Heartland's then-existing security situation or the SQL attack, which is the basis for Plaintiffs' fraud claims. (*See id.* at ¶ 107.) The statements have nothing to do with whether security is a "major driver" of Heartland's interests, and even if they did, they would not be misleading. As discussed above, allegations that Heartland had certain security problems do not by themselves support an inference that Heartland did not take the issue of data security seriously.

C. *Did Defendants' Statements Concerning the General State of Security at Heartland Trigger a Duty to Disclose the SQL Attack?*

Plaintiffs also argue that, even if Defendants' affirmative statements concerning the state of data security at Heartland are not in themselves misleading, those statements created a duty to disclose the SQL attack. In general, an omission is only fraudulent in the presence of a duty to disclose, which usually arises "only when there is insider trading, a statute requiring disclosure, or an inaccurate, incomplete, or misleading prior disclosure." *Winer Family Trust v. Queen,* 503 F.3d 319, 329 (3d Cir.2007). One affirmative statement does not automatically create a duty to simultaneously disclose all related material information. Rather, an affirmative statement will only create a duty to disclose additional facts if additional disclosures are required to make the affirmative statement not misleading. *See id.* (citing *Brody v. Transitional Hospitals Corp.,* 280 F.3d 997, 1006 (9th Cir.2002)); *Blackman v. Polaroid Corp.,* 910 F.2d 10, 16 (1st Cir.1990) (en banc)).

In this case, none of the allegedly fraudulent statements were rendered misleading by Defendants failure to disclose the SQL attack. Heartland's 10–K only sought to describe how Heartland's security system functioned in a general way; the report did not imply that Heartland had never experienced any security problems. (*See* Compl. at ¶ 95.) Therefore, the failure to disclose the SQL attack was not misleading in that context. Similarly, the statements on the November 4 conference call only dealt with Heartland's intention to pursue certain security measures in the future. (*See* Compl. at ¶ 106.) These statements did not become misleading just because Heartland did not disclose past security incidents that might or might not have been relevant to the company's decision to pursue new security measures. The Court does not deny the fact that knowledge of the 2007 breach might have been material to Plaintiffs' investment decisions. If Plaintiffs had known of the SQL attack, they might not have purchased Heartland securities. However, there is no general duty on the part of issuers to disclose every material fact to investors. *In re Burlington Coat Factory Sec. Litig.,* 114 F.3d 1410, 1432 (3d Cir.1997). Since Defendants are not alleged to have made any misleading statements, they never had a duty to disclose the 2007 breach.

***7** In sum, the Complaint does not identify any material misrepresentations or omissions. The statements Plaintiffs identify do not paint a misleading picture of Heartland's security systems. Defendants were never asked whether they suffered a security breach in late 2007, and the existence of such a breach does not make any of Defendants' statements concerning their security systems misleading. The Complaint therefore fails to allege one of the essential elements of a securities fraud claim and must be dismissed.

III. *Scienter*

To the extent that Plaintiffs' claims rest on allegations that Defendants misrepresented the general state of security at Heartland,[3] the Complaint is additionally deficient because it fails to allege scienter. To survive a motion to dismiss, the Complaint must allege facts sufficient to support an inference that Defendants made statements with knowledge that they were false or with recklessness as to whether or not they were false. *Avaya,* 564 F.3d at 267. Simply put, Plaintiffs do not allege that Defendants knew or had reason to suspect that Heartland's security systems were so deficient that it was false to say that Heartland "place[s] significant emphasis on maintaining a high level of security." (*See* Compl. ¶ 95.) According to the Complaint, the only people at Heartland who believed that the company had not adequately addressed the SQL attack were the former Senior Developer quoted above, another Senior Developer named George Duke, and a former Business Analyst. (*Id.* at ¶¶ 77–83.) Furthermore, none of these people are alleged to have expressed any reservations about security until after the credit card theft was discovered in January 2009. (*Id.*) This after-the-fact speculation by a handful of lower-level employees does not support the inference that Heartland and its corporate officers were consciously or recklessly dissembling when they stated that the company treated security as one of its central concerns.

Plaintiffs seek to bolster their scienter allegations by appealing to what they call the "core business

doctrine"—the idea that facts concerning a company's core business will be imputed to corporate officers. However, the cases to which Plaintiffs cite do not establish a rule of law. They simply confirm the uncontroversial proposition that a person's status as a corporate officer, when considered alongside other allegations, can help support an inference that that person is familiar with the company's most important operations. In other words, it is not automatically assumed that a corporate officer is familiar with certain facts just because these facts are important to the company's business; there must be other, individualized allegations that further suggest that the officer had knowledge of the fact in question. *See, e.g., In re Advanta Corp. Sec. Litig.,* 180 F.3d 525, 539 (3d Cir.1999); *In re Bio–Technology General Corp. Sec. Litig.,* 380 F.Supp.2d 574, 596 (D.N.J.2005).

***8** Taking into account the Complaint in its entirety, this Court finds that Plaintiffs have not alleged facts sufficient to support an inference that Defendants knew that Heartland was not paying proper attention to its security problems. The allegations do not create the impression that there was any kind of widespread concern that Heartland had not adequately addressed the SQL attack. Therefore, even if there were a handful of lower-level employees who were worried about ongoing problems created by the attack, there is nothing in the Complaint that supports an inference that these concerns were ever relayed to any of the Defendants. And if the Defendants lacked knowledge of any ongoing security problems at Heartland, they could not have acted with the requisite culpability when they claimed that Heartland was taking the issue of data security seriously. Since the Complaint does not adequately allege scienter, it must be dismissed.

It is worth noting that the Complaint at times appears to conflate knowledge of the SQL attack with the belief that Heartland faced ongoing security problems as a result of the attack. Assuming that Defendants were aware of the SQL attack, it does not follow necessarily that they believed that Heartland's security systems were deficient or that any problems created by the SQL attack had not been addressed. The Complaint contains no allegations—beyond bare awareness of the SQL attack—that support an inference that Defendants believed Heartland had serious ongoing security problems.

## *CONCLUSION*

Since Plaintiffs have failed to allege the existence of a material misstatement or omission, the Complaint fails to state a claim upon which relief may be granted. To the extent that the Complaint rests on allegations that Defendants misrepresented the general state of security at Heartland, the Complaint is additionally deficient because it fails to allege scienter adequately. Since these failures alone warrant dismissal, the Court will not reach the further questions of whether the Complaint adequately alleges loss causation or whether any of Defendants' statements fall within the PSLRA safe-harbor provision for forward-looking statements.

The Complaint will be DISMISSED. It appearing that further specificity would not cure the Complaint's deficiencies, amendment would be futile, so the dismissal will be with prejudice. An order to that effect will follow this opinion.

### All Citations

Not Reported in F.Supp.2d, 2009 WL 4798148

### Footnotes

1 A technical understanding of how a structured query language attack works is not necessary in this case. It suffices to say that the attack enabled hackers to inject foreign code into Heartland's computer systems.

2 This conclusion is buttressed by the full transcript of the earnings call, which Defendants attached as Exhibit D to their Motion to Dismiss. A court ordinarily only considers the Complaint in deciding a motion to dismiss, but when the Complaint relies on other documents, the court may consider those documents as well. *In re Burlington Coat Factory,* 114 F.3d, 1410, 1426 (3d Cir.1997) ("[A] 'document *integral to or explicitly relied* upon in the complaint' may be considered 'without converting the motion [to dismiss] into one for summary judgment.' ") (quoting *Shaw v. Digital Equipment,* 82 F.3d 1194, 1220 (1996)). Since the Complaint relies heavily and extensively on excerpts from the February 13 conference call, this Court has examined the full transcript to ensure that it fully understands the meaning of Defendants' statements.

3 As discussed in Part II, Plaintiffs allege two general types of fraud—fraudulently *omitting* to disclose the 2007 SQL

  

attack and fraudulently *affirmatively misrepresenting* the general state of security at Heartland. This opinion addresses scienter only as it pertains to the latter of these two categories—the affirmative misrepresentations.

**End of Document**