# Securities Fraud Class Action Suits Following Cyber Breaches: The Trickle Before the Wave

December 21, 2017

## Overview

Large-scale data breaches can give rise to a host of legal problems for the breached entity, ranging from consumer class action litigation to congressional inquiries and state attorneys general investigations. Increasingly, issuers are also facing the specter of federal securities fraud litigation.[1]

The existence of securities fraud litigation following a cyber breach is, to some extent, not surprising. Lawyer-driven securities litigation often follows stock price declines, even declines that are ostensibly unrelated to any prior public disclosure by an issuer. Until recently, significant declines in stock price following disclosures of cyber breaches were rare. But that is changing. The recent securities fraud class actions brought against Yahoo! and Equifax demonstrate this point; in both of those cases, significant stock price declines followed the disclosure of the breach. Similar cases can be expected whenever stock price declines follow cyber breach disclosures.

The claimed damages associated with a putative securities class action can be catastrophically large—driven by the size of the stock price decline and the volume of trading in an issuer's stock. The risks associated with such cases are therefore significant. But there are also a number of ways to successfully defend against them, both at the motion to dismiss phase—before issuers are exposed to the expense and distraction of discovery—and, if necessary, at later stages in the case.

As explained below, issuers should be thinking proactively about this risk. A company can strengthen its defense and help to protect itself against securities class action litigation by carefully attending to disclosure issues ***before*** any disclosure of a cyber breach and, indeed, before a breach ever happens. While companies will not be able to eliminate completely the risk of being subject to a securities fraud action related to cyber security, careful attention to these issues may reduce the risk, increase the possibility of early dismissal of such actions, and/or mitigate the potential scope of damages and costs associated with defending the litigation.

## Emerging Theories of Liability in Cyber Breach Securities Fraud Litigation

While each cyber breach may be unique, the core facts in these claims tend to follow a similar pattern. First, a company suffers a cyber-attack that leads to the theft of sensitive data. There is some delay between the company's detection of the breach and its disclosure to the market. After the disclosure, the company's stock price falls. Plaintiffs then allege that the drop in the stock price reflects the disclosure of some previously undisclosed fact.

In the typical case, plaintiffs allege two distinct theories of liability: (1) that the issuer's ***pre-breach*** statements failed to adequately disclose the risk of a breach or misrepresented the strength of its security

[1] Recent securities fraud class actions based on cyber-attacks include: *Sgarlata v. Paypal Holdings, Inc.*, No. 3:17-cv-06956 (N.D. Cal.); *In re Yahoo! Inc. Secs. Litig.*, No. 5:17-cv-00373-LHK (N.D. Cal.); *Brock v. Equifax Inc.*, No. 1:17-cv-04510 (N.D. Ga.); *In re Heartland Payment Sys. Sec. Litig.*, No, 09-1043, (D. N.J. December 7, 2009); *Ramnath v. Qudian Inc.*, No. 1:17-cv-9741 (S.D.N.Y.).

systems and commitment to security more generally and (2) that the company improperly withheld information about the breach ***after it was detected***. These theories are really two separate securities fraud claims, melded together by plaintiffs: one for those individuals who bought the stock before the breach and another for individuals who bought after the breach occurred but before it was publicly announced.

While each case will turn on its own specific facts, claims asserting a failure to adequately disclose a risk ***pre-breach*** or challenging general representations about the strength of a company's cybersecurity systems should be, depending on the nature of the alleged misstatements and the company's related risk disclosures, susceptible to strong motions to dismiss. This is particularly true for claims under the Securities Exchange Act of 1934 because, absent extraordinary circumstances, plaintiffs will have difficulty alleging scienter with the requisite specificity to survive a motion to dismiss on such claims.[2]

Claims based on assertions that a company improperly withheld information for some period of time ***after*** a breach was detected will likewise depend on the specific facts of the case. Plaintiffs may assert claims based on allegations that the company either provided inaccurate information about the breach or failed to disclose (i.e., omitted) material information. As to omissions, a company is not liable for an omission absent a duty to disclose, even if that omission is material. This principle led to the dismissal of an early cyber-breach case, *In re Heartland Payment Systems, Inc. Securities Litigation*. The court there dismissed the complaint in part because it found that the issuer was under no duty to disclose an initial cyber-attack, even though this information would have been material to investors.[3] Plaintiffs, of course, often seek to impose a duty to disclose omitted information by alleging either that the omission rendered affirmative statements made by the company misleading or by looking to other sources of law that they might argue impose such a duty. In any event, it would be prudent for a company to consider any potential disclosure obligations to which it may be subject, regardless of whether the company has an affirmative duty to disclose a known breach as a matter of the federal securities laws. Even if plaintiffs are able to point to an actionable material misstatement or omission, they must still clear the high bar of alleging scienter with the specificity required by the Private Securities Litigation Reform Act.

Notably, as in the anticorruption context, defendants may face challenges to statements of opinion about the strength of the company's security systems and controls, the company's commitment to compliance with applicable cyber-security law, or the company's commitment to security more generally under the standard set forth by the U.S. Supreme Court in *Omnicare, Inc. v. Laborers District Council Construction Industry Pension Fund*. This risk will be particularly acute in instances where the company discovers that a breach may have occurred (or has actually occurred) and makes public statements of opinion regarding the strength of its systems before disclosing the breach.

## Key Considerations for Issuers

### Pre-Breach Statements

Typically, plaintiffs who seek to assert claims for statements made prior to a breach focus on statements touting a company's cybersecurity regime and general statements about the company's commitment to data security. In order to minimize the risk of claims based on statements made before a breach has occurred, issuers should consider taking steps to protect themselves by, for example, reviewing their existing disclosures to ensure that they are properly aligned with the issuer's actual risk profile and

[2] Because scienter is typically not an element of claims brought under the Securities Act of 1933, defenses based on scienter may well be unavailable in connection with such cases.

[3] *Heartland*, No, 09-1043, Opn. at 11 (D. N.J. December 7, 2009).

circumstances. Carefully crafted and robust risk disclosures can go far in foreclosing liability for statements made before any breach has occurred. It is also worth considering whether any affirmative statements about the company's systems, their relative strength or the company's commitment to monitoring, improving and enhancing its cyber security protections are necessary and advisable in the first instance.

### Post-Breach Statements and Omissions

In most cases, the critical period for securities liability will be the time between the company's detection of the breach and its public disclosure of the breach. If the breach is substantial enough that it will have to be disclosed, then potential damages in a possible securities fraud action may increase with each day an issuer delays its disclosure of the breach. Moreover, if the breach is not communicated and understood throughout the company, additional events may occur and later be seized on by plaintiffs. For example, in the *Equifax* case, the fact that insiders, including the CEO, sold nearly $2 million worth of Equifax stock two days after the company discovered the breach (but before it was publicly disclosed)[4] allowed plaintiffs to allege that those defendants had a motive to commit fraud, which can be used by plaintiffs as evidence of scienter. The motive in the *Yahoo!* case was alleged to have been even broader: plaintiffs claimed that the company first concealed the hack in an effort (1) to shore up Yahoo!'s deteriorating financial performance (alleging that the company assumed that its users would defect if they knew that their data was not secure), and later (2) to ensure that the sale of Yahoo!'s core business to Verizon would proceed.

Because the actions a company takes upon learning of a breach can have serious ramifications in subsequent securities litigation, companies should be proactive in thinking about how they would handle a breach if it were to occur. Developing and practicing an incident response plan in advance of any breach will allow the company to consider the steps that will need to be taken, thereby minimizing the risks associated with a rushed reaction. And in the event that a breach occurs, it will be important that the company seriously consider disclosure questions on an ongoing basis, including the timing and scope thereof.

### Monitoring and Internal Reporting

One recurring factor about cyber events is that a company may not even know that a breach has occurred, or it may not fully understand the scope or severity of the breach for some period of time. For that reason, companies often wait days or weeks before making a public disclosure about a breach, in order to allow time for the company to investigate and to make the complex decisions about communications to insurers, auditors, customers, regulators and the market. While understandable, plaintiffs' firms are likely to challenge this delay in the class action securities context, especially where company officers make public statements during the interim period. For this reason, it is important for companies to have appropriate monitoring and reporting lines in place to detect breaches and alert senior management as quickly as possible. A company that falls victim to a cyber breach can significantly mitigate its exposure to securities fraud class actions by promptly assessing the scope and severity of the breach and quickly reaching decisions on how to carry out any applicable reporting obligations.

[4] The insider stock sales in Equifax were not made pursuant to a 10b5-1 scheduled trading plan, but Equifax's internal investigation established that the executives were unaware of the breach..

Davis Polk

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.


| | | |
|---|---|---|
| **Michael S. Flynn** | **212 450 4766** | **michael.flynn@davispolk.com** |
| **Avi Gesser** | **212 450 4181** | **avi.gesser@davispolk.com** |
| **Edmund Polubinski III** | **212 450 4695** | **edmund.polubinski@davispolk.com** |
| **Neal A. Potischman** | **650 752 2021** | **neal.potischman@davispolk.com** |
| **Brian S. Weinstein** | **212 450 4972** | **brian.weinstein@davispolk.com** |
| **Joseph A. Hall** | **212 450 4565** | **joseph.hall@davispolk.com** |