Cybersecurity Law Report
An Acuris company

cslawreport.com

February 13, 2019

CLASS ACTIONS

Reducing Risk in the Dawn of Equifax and Other Cyber-Related Securities Fraud Class Actions

By Avi Gesser, Patrick Blakemore and Peter Bozzo, *Davis Polk*

Public companies face a variety of legal challenges following major cyber events: consumer class actions, inquiries from regulators (*e.g.*, state attorneys general, SEC, NYDFS, CFTC, FTC), congressional inquiries and, increasingly, federal securities class actions. In consumer class actions arising from data breaches, the potential damages sustained by people whose information was compromised are usually small, if there are any damages at all. But federal securities class actions can expose public companies that experience cyber events to very significant claims for damages from plaintiff shareholders – damages that are driven, in rough terms, by the size of the stock-price decline following the public disclosure.

Until recently, such price declines were rare, and the viability of shareholder suits resulting from a company's cyber breach was uncertain – but that may be changing. The recent securities fraud class actions brought against Yahoo!, PayPal, Chegg and Marriott, and in particular, the January 28, 2019, decision in *In re Equifax Securities Litigation*, which allowed most of plaintiffs' claims to survive a motion to dismiss, are cause to give these cases a closer look.

As discussed below, the Equifax decision illustrates that, in certain circumstances, these cases present risk and may have viability beyond the motion to dismiss stage, but it also shows that there are several steps that companies can take to (1) reduce the risk of such cases being filed, (2) increase the possibility of early dismissal of such actions, and (3) mitigate the potential scope of damages and costs associated with defending and resolving them.

See "Defense and Plaintiff Perspectives on How to Survive Data Privacy Collateral Litigation" (Mar. 8, 2017).

Emerging Theories of Liability in Cyber Breach Securities Fraud Litigation

While each cyber breach is unique, the core facts in cyber-related securities fraud cases tend to follow a similar pattern:

1. A company makes statements about its data security policies and procedures.

2. The company subsequently suffers a cyber event that results in the loss of sensitive, non-public data.
3. There is some delay between the cyber event and the company's detection of the event.
4. There is some delay between the company's detection of the event and its disclosure of the event to the market.
5. Immediately after the disclosure, the company's stock price falls by a significant amount.
6. Plaintiffs file suit alleging that the drop in stock price resulted from disclosure of some previously undisclosed fact related to the cyber event.

Based on this increasingly common sequence of events, plaintiffs generally allege two theories of liability. First, plaintiffs allege that the issuer's statements before the breach misled investors regarding the strength of its cybersecurity systems and its commitment to data privacy. Second, plaintiffs contend that the company was too slow to disclose the breach after it was detected, thereby misleading investors. While plaintiffs often conflate these theories, they raise two distinct securities fraud claims that correspond to two distinct classes – one for shareholders who bought stock after an affirmative pre-breach statement about the company's cybersecurity and another for those who bought after the breach but before the public disclosure.[1]

See "Minimizing Class Action Risk in Breach Response" (Jun. 8, 2016).

Equifax Class Action Securities Claims Survive

Following Equifax's disclosure of a large data breach in September 2017, its stock price declined by nearly 36 percent, and a purported class of shareholders soon thereafter brought a claim under Section 10(b) of the Securities Exchange Act. The plaintiffs alleged that Equifax made misrepresentations in SEC filings, on its website and during investor conferences related to "the strength of Equifax's cybersecurity systems, its compliance with data protection laws, and the integrity of its internal controls." Plaintiffs claimed that, in spite of these representations, Equifax's cybersecurity systems were "dangerously deficient" and that Equifax "failed to meet the most basic industry standards" by storing sensitive data on public-facing servers, failing to encrypt sensitive information and using inadequate network-monitoring procedures.

On June 7, 2018, Equifax and four of its executives moved to dismiss those claims on the grounds that plaintiffs had not adequately alleged false or misleading statements, scienter or loss causation. On January 28, 2019, District Judge Thomas W. Thrash, Jr., denied the motion to dismiss filed by Equifax and its CEO, and allowed the plaintiffs' claims against those defendants to move forward. The court granted the motion to dismiss with respect to the other individual defendants.

See "Lessons From the Equifax Breach on How to Bolster Incident Response Planning (Part One of Two)" (Sep. 27, 2017); Part Two (Oct. 11, 2017).

Pleading Scienter and Loss Causation

In general, there are two elements of class-action securities claims relating to cyber events that pose high pleading thresholds and thus render those claims particularly vulnerable to dismissal: scienter and loss causation. To plead their claims, plaintiffs asserting Section 10(b) claims must "state with particularity facts giving rise to a strong inference that the defendant acted with the required state of mind" – *i.e.*, scienter – and, for allegations regarding any material statements or omissions that are "made on information and belief," must "state with particularity all facts on which that belief is formed." Plaintiffs often have particular difficulties obtaining the information necessary to plead scienter in these cases because the Private Securities Litigation Reform Act requires courts (with minimal exceptions) to stay discovery during the pendency of a motion to dismiss.

Separately, to sufficiently plead loss causation, a plaintiff must "show that a misrepresentation that affected the integrity of the market price also caused a subsequent economic loss." This element can prove to be a significant hurdle for class-action securities fraud claims. In *Dura Pharmaceuticals, Inc. v. Broudo*, the Supreme Court held that to establish this element, plaintiffs must do more than show that "the price on the date of purchase was inflated because of the misrepresentation." The court then held that the plaintiffs failed to state a claim because they did not "provide the defendants with notice of what the relevant economic loss might be or of what the causal connection might be between that loss and the misrepresentation."

See "The New Normal: Easier Data Breach Standing Is Here to Stay" (Feb. 6, 2019).

An Outlier?

Equifax marks the first time a plaintiff's scienter and loss causation allegations have survived a motion to dismiss in a cyber-related securities class action. The court held that "it was false, or at least misleading, for Equifax to tout its advanced cybersecurity protections" in spite of "the dangerously deficient state of Equifax's cybersecurity." The court went on to hold that plaintiffs had cleared the high bar for pleading scienter as to Equifax and its CEO, in part based on the allegation that the CEO had overseen an investigation in the wake of a prior breach that revealed the weaknesses of Equifax's systems. Notably, however, the court held that plaintiffs had failed to offer particularized allegations sufficient to support a strong inference of scienter as to the other three individual defendants.[2]

It remains to be seen whether *Equifax* is an outlier on the scienter issue. Following the public disclosure of the Equifax breach, there were congressional hearings, public statements and media reports that provided plaintiffs with the details needed to plead scienter that would not normally be available to plaintiffs absent discovery. In other situations – the *PayPal* case, for example – the lack of specific factual allegations regarding the alleged contrary knowledge of company officers resulted in a conclusion that plaintiffs' scienter allegations were insufficient to sustain a federal securities fraud claim.

Heightened Pleading Not Required

The *Equifax* court also held that loss causation is not governed by a heightened pleading standard (contrary to the rule adopted by some other circuits)[3] and went on to hold that plaintiffs had adequately pleaded loss causation by suggesting that Equifax's disclosures about the breach and its poor cybersecurity protections had led to its stock decline. Defendants had argued that "the most rational inference is that Equifax's stock price declined [following the disclosure] due to concerns about the cost and impact of the additional investigations and continued negative publicity rather than as a result of a revelation of 'fraud.'"

Key Steps for Minimizing Risk

The number of class action securities cases arising out of data breaches – and the costs to resolve them – rose dramatically in 2018 and will likely continue to rise in 2019, but there are several things that companies can do to reduce the risks posed by these suits.

Ensure Pre-Breach Statements Are Accurate

Typically, following a major data breach, plaintiffs look to assert claims based on statements that the company made prior to the breach that emphasized its cybersecurity and commitment to data privacy. To minimize the risk of claims based on these kinds of statements, issuers should not only scrutinize the accuracy of such statements when they are made, but also assess whether those statements are likely to remain accurate in the face of potentially unknowable developments. For example, companies may want to avoid stating that they have never been the victim of a successful hack because there may be breaches that they are not aware of, and they may want to avoid the disclosure issues that would arise if something later happens that renders those statements no longer accurate. Issuers should also ensure that their statements on cybersecurity and data privacy include appropriate caveats and risk disclosures, and avoid unqualified definitive language such as "our cybersecurity is fully consistent with industry best practices" or "we do everything we can to protect our customers' data."

Address Post-Breach Statements in Incident-Response Planning

A critical period for securities liability is the time between the company's detection of the breach and its public disclosure. Mindful of the possibility of post-breach securities fraud claims, public companies should be forward-thinking in crafting and testing their incident-response plans in order to be prepared for a potential breach. The actions that a company takes upon learning of a breach often have critical ramifications for subsequent litigation.

Plaintiffs may assert claims based on allegations that the company made misleading statements about its data security in light of the breach, provided inaccurate information about the breach itself, or failed entirely to disclose the breach even though it was material. As to the failure to disclose claim, courts have held that an issuer is under no duty to disclose an initial cyber-attack, even

though this information would have been material to investors, absent a duty to disclose. Plaintiffs therefore seek to impose such a duty either by alleging that the omission rendered the company's other affirmative statements misleading or by looking to other sources of law that might impose a duty to disclose.

For example, in *In re Yahoo! Inc. Securities Litigation* – which eventually settled for $80 million – plaintiffs claimed that the company concealed one of the hacks against it for over two years 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 (2) later, to ensure that the sale of Yahoo!'s core business to Verizon would proceed uninterrupted. During that period, Yahoo! filed quarterly and yearly reports with the SEC stating that cyber breaches posed a major threat to its operations without disclosing that such a breach had actually occurred – disclosures that the SEC found were misleading.

Equifax made a series of disclosures about the breach beginning more than five weeks after it was discovered, and the amended complaint referred to those disclosures in detail in an attempt to allege that Equifax mishandled the remediation efforts and that these failures tainted the company's cybersecurity compliance more broadly. The court dismissed the post-breach claims in Equifax, holding that Equifax had no duty to disclose that a breach had occurred. Although plaintiffs alleged that the occurrence of a breach rendered Equifax's previous representations about its security systems misleading, the court rejected that argument: Because "the occurrence of a data breach does not necessarily imply that a company's data security is inadequate," the Equifax breach "did not necessarily render the [d]efendants' prior statements false[] and thus did not impose a duty to correct those statements by disclosing the occurrence of the [d]ata [b]reach."

In the event that a breach occurs, a company must consider questions about the timing and scope of its disclosures on an ongoing basis, especially with respect to its next quarterly public filings. Companies should also consider their disclosure obligations under federal reporting requirements and state laws governing reporting of cybersecurity issues.

See "Ten Common Post-Breach Public Relations Failures and How to Avoid Them" (Apr. 18, 2018).

Ensure Appropriate Monitoring and Internal Reporting

In many cyber events, a company may not even know whether data has been accessed or stolen (or may not fully understand the scope or severity of the breach) for some period. For that reason, companies often wait days or weeks before making a public disclosure about a breach, thinking that the delay will give the company time to investigate and make decisions about communications to insurers, auditors, customers, regulators and the market. While this instinct is understandable, plaintiffs' firms are likely to challenge any disclosure delays when they bring class action securities complaints, especially where the company or its officers make public statements about cybersecurity during the interval between the breach and its disclosure. In this respect, following a cyber event, companies should carefully consider on an ongoing basis both (1) potential regulatory and contractual disclosure obligations to which they may be subject, regardless of whether

they have an affirmative duty to disclose a known breach as a matter of federal securities law, and (2) the legal and strategic implications and risks associated with the various options for the timing and scope of disclosure, including the option not to disclose. To do this effectively, companies should have appropriate monitoring and reporting lines in place to detect breaches and alert senior management promptly once a breach has occurred. This will allow senior management to consider its disclosure obligations and to address insider trading risks as quickly as possible.

Avi Gesser is a partner in Davis Polk's litigation department, representing clients in a wide range of cybersecurity issues and counseling companies that have experienced cyber events. He is a frequent writer and commentator on cybersecurity issues.

Patrick Blakemore is an associate in Davis Polk's litigation department.

Peter Bozzo is an associate in Davis Polk's litigation department.

[1] These theories can be applied to cyber issues that companies face besides actual breaches, such as the disclosure of a previously unknown vulnerability or security flaw. For example, see Consolidated Class Action Complaint for Violations of the Federal Securities Laws, *In re Intel Corp. Sec. Litig.*, No. 18-cv-00507-YGR (N.D. Cal.) (filed July 10, 2018), ¶¶ 42–43.

[2] The court specifically found that various factors – such as the egregiousness of Equifax's cybersecurity deficiencies, sales of stock by its top executives in the days after the breach, and the sudden resignations of top executives—were insufficient, standing on their own, to establish scienter. *Id.* at *26–*29.

[3] *See Ore. Pub. Emps. Ret. Fund v. Apollo Grp. Inc.*, 774 F.3d 598, 605 (9th Cir. 2014) ("Rule 9(b) applies to all elements of a securities fraud action, including loss causation."); *Katyle v. Penn Nat'l Gaming, Inc.*, 637 F.3d 462, 471 (4th Cir. 2011) ("We review allegations of loss causation for 'sufficient specificity,' a standard largely consonant with Fed. R. Civ. P. 9(b)'s requirement that averments of fraud be pled with particularity.").