WINSTON & STRAWN LLP

CLIENT ALERT

Plaintiffs Increasingly Pursuing Class Action Securities Fraud Claims Following Data Breaches

JANUARY 30, 2018

Uptick in Direct Action Securities Fraud Complaints

In the last few months, there have been a number of class action federal securities fraud complaints filed against companies that have disclosed data breaches or electronic information security vulnerabilities. In the past, well-publicized breaches triggered primarily shareholder derivative, state consumer protection, and common law actions. With some exceptions, most of those breaches did not lead to class action securities fraud claims—most likely because they did not precipitate meaningful stock price drops. Recent data breach disclosures, however, have been accompanied by relatively larger price drops, and thus, putative shareholder class action fraud suits asserting alleged violations of Section 10(b) of the Securities Exchange Act of 1934 and SEC Rule 10b-5, or in the case of plaintiffs that are able to connect their suit to a recent public securities offering, alleged violations of Sections 11 and/or 12(a)(2) of the Securities Act of 1933. *See, e.g., Kuhns v. Equifax Inc.*, No. 1:17-cv-03463-TWT (N.D. Ga.) (complaint filed Sept. 8., 2017 following alleged approximately 16.8% stock price drop); *Sgarlata v. Paypal Holdings, Inc.*, No. 3:17-cv-06956 (N.D. Cal.) (complaint filed Dec. 6, 2017 following alleged 5.75% stock price drop); *Ranmath v. Qudian*, No. 17-cv-9741 (S.D.N.Y.) (complaint filed Dec. 12, 2017 following alleged 45% drop in price of depositary shares); *Alvira v. Intel Corp.*, No. 2:18-cv-00223 (C.D. Cal.) (complaint filed Jan. 10, 2018 following alleged 3.5% stock price drop).

The plaintiffs in these complaints have generally attempted to fashion a fraud narrative by seizing upon statements made by the defendants concerning the issuing company's data security or internal controls in the past, when the securities were first offered publicly or were otherwise trading at a higher price, and asserting that the defendants' statements were misleading and thus inflated the public stock price. Plaintiffs then compare those statements to the more recent, negative news—i.e., news of a data hack or revelation of an information security weakness—that allegedly corrected or revealed a truth that was concealed or misrepresented by the prior statements, removing the stock price inflation and precipitating a price drop. The plaintiffs argue that, prior to the breach, the defendants misrepresented the strength of the company's data security or minimized its susceptibility to breach; and/or that, after becoming aware of the breach or security vulnerability, the defendants misleadingly concealed or downplayed the nature of that breach or vulnerability. The latter theory, if factually supported, appears more likely to stand up to pre-discovery motion practice and generate litigation carrying potentially substantial exposure for issuers.

Certain Plaintiffs' Theories and Defense Arguments Are Likely to be Tested

Plaintiffs asserting Section 10(b) claims in this context will likely be subject to Rule 12(b)(6) motion practice on the grounds that they do not adequately allege the defendants' scienter with the factual specificity required by the Private Securities Litigation Reform Act ("PSLRA"), 15 U.S.C. §§ 78u-4(b). In cases involving an alleged pre-breach misrepresentation concerning a company's susceptibility to breach, unless the plaintiff has the unusual benefit of detailed confidential witness allegations or publicized findings stemming from a regulatory investigation, for example, motions to dismiss based on scienter could prove a powerful early weapon for issuers defending against these types of suits.

Complaints that assert Securities Act claims likely will not face the hurdle of pleading scienter, but may be subject to motions to dismiss based on failure to allege falsity (as will also be the case for Section 10(b) claims)—again, particularly as to alleged pre-breach misrepresentations—unless they are able to point to specific statements on the issue of data security that have proved to be untrue at the time they were made. It might not be enough for plaintiffs to point to company filings or releases that did not expressly disclose a potential vulnerability or security risk, as companies typically are not required to disclose information—even if material—absent a particular duty to disclose. *See Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011).[1] Additionally, depending on the nature of the claim asserted, statements made by the company as to the quality of its data security may constitute opinions, which are actionable only in delineated circumstances, *see Omnicare, Inc. v. Laborers Dist. Council Construction Indus.*, 135 S. Ct. 1318 (2015); or, if accompanied by adequate cautionary language, may qualify for protection under the judicially recognized "bespeaks caution" doctrine, *see Luce v. Edelstein*, 802 F.2d 49, 56 (2d Cir. 1986), or fall within the PSLRA safe harbor from liability for forward-looking statements. 15 U.S.C. § 78u-5(c). Perhaps more complicated will be claims that the issuer was aware of a breach or vulnerability but delayed in bringing it to the attention of the public, such that post-breach statements that failed to disclose that information were materially misleading.

Ultimately, as noted in an early class action securities fraud case that was brought in the wake of a data hack against Heartland Payment Systems, Inc., a bank card payment processor, "careful attention to context" may not demonstrate that the defendants' alleged misrepresentations are not actionable according to some or all of the above defenses. *See In re Heartland Payment Sys., Inc. Sec. Litig.*, 2009 WL 4798148, Civ. No. 09-1043, at *3, *4-8 (D.N.J. Dec. 7, 2009) (granting motion to dismiss fraud claims under the Exchange Act alleging that the defendants concealed the data hack and misrepresented the state of Heartland's data security, finding that the plaintiffs failed to adequately allege falsity, including because the defendants had no duty to disclose the initial hack, and additionally failed to sufficiently plead scienter).

Proactive Issuer Measures to Reduce Exposure

The uptick in securities fraud claims stemming from data breaches seems likely to emerge as a trend in the face of continued public consciousness, investor sensitivity, and regulatory scrutiny concerning personal data privacy and security. Expect these complaints to strengthen, as well, as plaintiffs obtain the benefit of publicized regulatory allegations or findings, support from confidential witnesses (particularly where data breaches result in employee terminations or reorganizations), or additional indicia of scienter through well-timed insider stock sales.

In the current climate, there are a number of ways in which a company can position itself to best defend against a potential securities fraud claim in the wake of a data breach or disclosed security vulnerability and minimize liability, including:

- Thoroughly assess the current state of the company's information security and privacy environment, and review how that environment is described internally as compared to the company's public descriptions of its information security environment, and determine whether updated or supplemental disclosures would better describe the company's current systems;

- Review the company's risk disclosures concerning data security and potential unintended disclosure of sensitive personal or other secured information, and modify and/or enhance those disclosures in the future as appropriate (i.e., through greater specificity or cautionary language) to increase the likelihood that a court examining those disclosures will apply doctrines that shield them from fraud liability;
- Give consideration to what, if any, data security-related disclosure obligations the company might be subject now or in the event of a breach, including identifying, as may be appropriate, a threshold severity of breach needed to trigger disclosure—not just to the public, but to regulators or other constituents;
- Plan ahead and develop procedures for mitigating and reacting to a potential breach, including escalation criteria and a clear decision-making protocol for whether and in what fashion to disclose a breach or identified vulnerability.

We will continue to monitor this space and provide updates. In the meantime, companies should undertake efforts to assess their privacy and data security programs, and to ensure alignment among individuals managing the companies' data privacy, information security, legal/disclosure, and media relations functions.

---

[1] The Supreme Court had been slated to potentially resolve a circuit split concerning whether an issuer may be liable for federal securities fraud for failing to disclose "known trends or uncertainties" as required by SEC Regulation S-K Item 303, even in the absence of a misleading statement on the subject in question. See Leidos, Inc. v. Indiana Pub. Ret. Sys., Dkt. No. 16-581. However, as of the date of this publication, the case had been held in abeyance and removed from the argument calendar pursuant to a pending settlement.

6 Min Read

Related Locations

Charlotte | Chicago | Dallas | Houston | Los Angeles | New York | San Francisco | Silicon Valley | Washington, DC

Related Topics

Class Action Litigation | Securities Litigation | Fraud Claims | Data Security | Data Breach

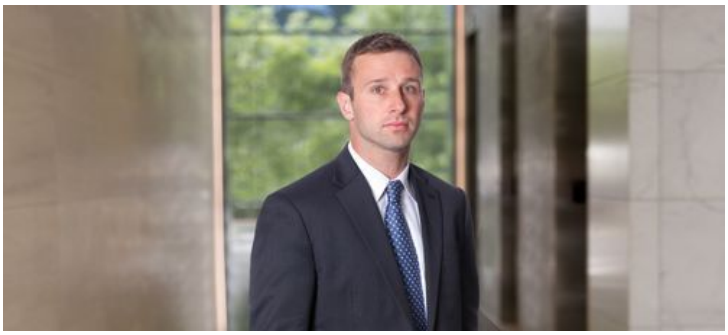
Related Capabilities

Litigation/Trials | Securities, M&A & Corporate Governance Litigation | Class Actions & Group Litigation | Privacy & Data Security | Compliance Programs | Trade Secrets, Non Competes & Restrictive Covenants

Related Regions

North America

Related Professionals



Steven Grimes

Joseph L. Motto

Thomas Weber