ALERT MEMORANDUM

Cyber Breaches: Lessons Learned from Shareholder Derivative and Securities Fraud Litigation

Overview

As the number and scale of data breaches in recent years have grown, the question for many companies is not *if* but *when* they will be compromised by a cybersecurity attack. In addition to responding to front-page headlines and trying to mitigate reputational harm, companies are required to navigate the shifting landscape of cybersecurity litigation and regulatory actions.

For years, practitioners have been predicting that cybersecurity breaches will bring a wave of shareholder derivative suits and securities fraud class actions. Yet plaintiffs pursuing such derivative litigation, generally against corporate directors and officers for breach of fiduciary duties in connection with data breaches, have fared poorly in the face of strong defenses regarding the pre-suit demand requirement and the protective standard of the business judgment rule. Shareholders seeking to pursue securities fraud litigation face a separate set of hurdles, given that disclosures of even large data breaches have not historically been accompanied by a significant decline in stock price.

While the future of cybersecurity derivative and securities litigation remains uncertain, there is reason to believe that the volume and success of such suits may be on the rise. With respect to shareholder derivative lawsuits, as cybersecurity issues become more ubiquitous, directors and officers will be increasingly on notice of data breach risks, and plaintiffs will more easily be able to argue that directors and officers should have been aware of the company's susceptibility to a cyberattack and should have taken efforts to remedy the company's vulnerabilities.

In the context of securities fraud litigation, there are a number of reasons to believe that disclosures of data breaches will increasingly have an impact on stock prices, including that investors are beginning to gain a better understanding of the risks and financial impact of data breaches and respond to them. Further, companies reacting to investor concerns regarding data security are likely to make more public statements regarding their commitment to cyber protections. Such statements will incorporate strong cybersecurity expectations into a company's stock price and, thus, may lead to a price decline in the face of a data breach. Recent securities fraud class actions brought against Yahoo and Equifax affirm this trend. In both cases, disclosure of a data breach was followed by a significant stock price drop.

While the success of shareholder derivative suits in the cybersecurity context remains an uphill battle, given plaintiffs' track record, and while the potential oncoming wave of securities fraud class actions is still in its nascent phases, the risks of such suits are nonetheless significant, given the public's increased focus on the issue and the possibility of enormous damages claims. Thus, there is good reason for companies to focus on cybersecurity and the accompanying litigation risks and take proactive steps, both prior to a breach and in the aftermath of one. This brochure explores recent shareholder derivative litigation and securities fraud class actions, highlighting lessons learned in order to assist companies in best positioning themselves to defend against the ever-growing possibility of such a lawsuit.

Shareholder Derivative Litigation

Dismissed Actions

Wyndham

On October 20, 2014, the District Court of New Jersey dismissed a shareholder derivative suit brought against the directors and officers of Wyndham Worldwide Corporation ("Wyndham") in the aftermath of a series of cybersecurity attacks, holding that the board's refusal to pursue litigation following a shareholder demand was a good-faith exercise of business judgment made after a reasonable investigation.[1]

The suit arose out of three breaches of Wyndham's online networks between April 2008 and January 2010, resulting in the theft of personal and financial information of over 600,000 customers and leading to subsequent legal action against the company on behalf of the Federal Trade Commission ("FTC"). Following the Wyndham board's refusal to pursue litigation, the plaintiff filed a derivative lawsuit, asserting claims for breach of fiduciary duty, corporate waste, and unjust enrichment. The plaintiff alleged that the board and management's failure to implement adequate data-security mechanisms to prevent the data breaches, and their failure to timely disclose the breaches, damaged the company's reputation and cost it significant legal fees.

Applying Delaware law, the court dismissed the suit, finding that the plaintiff failed to rebut the business judgment rule—that is, he failed to adequately plead that the Wyndham board's refusal of the plaintiff's demand was either (1) made in bad faith or (2) based on an unreasonable investigation.

The court identified several factors that were relevant to determining that Wyndham's directors and officers undertook a reasonable investigation in rejecting the plaintiff's demand, including: (1) the board, and separately the audit committee, discussed the cyberattacks, the company's security policies, and proposed security enhancements at a variety of meetings starting about six months after the initial breach; (2) the company hired third-party technology firms to investigate each breach and to issue recommendations regarding the company's security; and (3) the company began implementing the recommendations of the retained technology firms. The court concluded that the board "had a firm grasp" of the plaintiff's demand when it decided that pursuing litigation was not in the corporation's best interest but noted that "courts uphold even cursory investigations by boards refusing shareholder demands" given the

[1] *Palkon v. Holmes*, No. 2:14-CV-01234 (SRC), 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

business judgment rule's "strong presumption."[2] Further, in a footnote, the court commented that the merits of the underlying claims were also potentially weak because the company had implemented security measures prior to the first data breach and had addressed security concerns numerous times.[3]

This decision reinforces the difficulties plaintiffs face in overcoming the protections of the business judgment rule and the demand requirement. It also provides useful guidance regarding the type of proactive steps directors and officers can take in advance of and following a cybersecurity breach, including: (1) making data security a regular topic of discussion at board meetings; (2) designating a board committee to oversee the company's data security; (3) retaining outside consultants to evaluate the company's data protections and make recommendations for enhancements; and (4) taking proactive steps to address any vulnerabilities identified.

Target

In late 2013, Target suffered a significant data breach at the hands of sophisticated cyber criminals. The hackers infiltrated Target's systems and obtained the personal and financial data of millions of customers—including credit card and debit card records and encrypted PINs.[4] In response, various shareholders brought derivative actions in Minnesota district court against the company and certain of its officers and directors, alleging that Target's board and management had breached their fiduciary duties by failing to implement sufficient data protections and cybersecurity measures. The plaintiffs alleged that the defendants aggravated the damage by failing to provide prompt and accurate notice to consumers—Target disclosed the breach three weeks later, only after a third-party reported the incident, and allegedly initially concealed the full nature and scope of the breach.[5] Alleging severe damage to the company, the plaintiffs pointed to investigations by the Secret Service and the DOJ, as well as multiple class action lawsuits on behalf of aggrieved customers.[6]

In order to investigate the shareholders' allegations, and pursuant to Minnesota law, Target established an independent Special Litigation Committee ("SLC"), which conducted a more than 21-month investigation. With the assistance of independent counsel and experts, the SLC reviewed hundreds of thousands of documents and interviewed over 65 witnesses, and ultimately concluded in a 91-page report that Target should not pursue the derivative claims. The SLC took into account, among other things, Target's efforts to strengthen its security systems both before and after the breach and its efforts to assess and monitor compliance with security standards, including by engaging internal and external auditors and third-party consultants.[7]

Thereafter, the SLC and the defendants moved to dismiss the action, and the shareholder plaintiffs, faced with the committee's rigorous report, chose not to oppose the dismissal. In July 2016, in a two-page order, the district court dismissed the action, noting the plaintiffs' position.[8]

As with *Wyndham*, the court did not reach the merits of the derivative action but instead deferred to the company's decision not to pursue litigation on behalf of its shareholders. The case highlights the procedural hurdles that derivative plaintiffs face in simply establishing their right to bring a claim. It also provides another data point on the extent and type of investigation done by a company to determine whether to bring a derivative suit that withstood scrutiny in the aftermath of a massive data breach.

Home Depot

In November 2016, yet another cybersecurity-related shareholder derivative suit was dismissed for failure to overcome initial procedural hurdles, this time on the

[2] *Id.* at *6.

[3] *Id.* at *6 n.1.

[4] Verified Shareholder Derivative Complaint at 1-3, *Davis v. Steinhafel*, No. 0:14-cv-00203 (D. Minn. Jan. 21, 2014).

[5] *Id.* at 2-3.

[6] *Id.* at 3.

[7] Report of the Special Litigation Committee, *Steinhafel*, No. 0:14-cv-00203.

[8] Preliminary Order of Dismissal, *Steinhafel*, No. 0:14-cv-00203.

ground that the plaintiffs failed to plead demand futility. This case arose out of a 2014 breach of Home Depot's security systems that allowed hackers to capture customers' personal financial data every time a card was swiped at a cash register.[9] The breach allegedly continued undetected for nearly five months,[10] resulting in the theft of the financial data of over 56 million customers at a predicted total cost to the company, "after all is said and done," of almost $10 billion.[11]

In August 2015, shareholders brought a derivative action against Home Depot and certain of its officers and directors, alleging that the defendants breached their fiduciary duties by failing to employ reasonable measures and implement sufficient internal controls to oversee cybersecurity risks and protect customer data. On multiple occasions prior to the breach, the board was informed that Home Depot's security systems were inadequate and did not comply with industry standards. Although it had begun implementing a plan to update its security systems, the company's then-CEO acknowledged that the systems were still "desperately out of date" at the time of the breach.[12] The plaintiffs also alleged, among other things, that the defendants wasted corporate assets.

On November 30, 2016, the Northern District of Georgia dismissed the action based on the plaintiffs' failure to fulfill the demand requirement, rejecting the plaintiffs' argument that demand was futile. The court stated that, under Delaware law, in order for plaintiffs to meet the demand futility requirement with respect to their breach of loyalty claim, they must "show with particularized facts beyond a reasonable doubt that a majority of the Board faced substantial liability because it consciously failed to act in the face of a known duty to act."[13] The court noted that it is "not surprising" that the plaintiffs failed to overcome this "incredibly high hurdle."[14]

In response to the plaintiffs' argument that the board failed to immediately implement a plan to address known deficiencies in the company's data security system, the court acknowledged that in hindsight the board's implementation was "probably too slow" and likely inadequate, but that directors' decisions must only be "reasonable, not perfect."[15] To breach the duty of loyalty, directors must "knowingly and *completely*" fail to undertake their responsibilities; incorrectly exercising business judgment and making the "wrong decision in response to red flags" is not enough.[16]

With respect to the plaintiffs' claim that the company's insufficient reaction to cybersecurity threats wasted corporate assets, the court held that the decision to update the company's security "at a leisurely pace" "falls square within the discretion of the Board and is under the protection of the business judgment rule" even if the decision was "an unfortunate one."[17]

Following the district court's dismissal, the plaintiffs filed a notice of appeal. The parties, however, reached a settlement in which Home Deport agreed to adopt certain cybersecurity-related corporate governance reforms and pay $1.125 million of the plaintiffs' attorney's fees.

The district court's decision highlights that courts are willing to liberally extend business judgment protections and will not subject directors and officers to hindsight judgments. Nevertheless, the court made clear that doing *nothing* in the face of known security threats will not suffice. To ensure that their actions are protected, directors and officers should take reasonable and informed steps to ensure that security threats are addressed, both preemptively and in response to an actual breach.

[9] *In re the Home Depot, Inc. Shareholder Deriv. Litig.*, 223 F. Supp. 3d 1317, 1320 (N.D. Ga. 2016).

[10] Verified Shareholder Derivative Complaint ¶ 4, *In re the Home Depot, Inc. Shareholder Deriv. Litig.*, 223 F. Supp. 3d at 1320.

[11] *In re the Home Depot*, 223 F. Supp. 3d at 1321.

[12] *Id.* at 1322.

[13] *Id.* at 1325.

[14] *Id.*

[15] *Id.* at 1327.

[16] *Id.* at 1326-27 (citations and internal quotation marks omitted).

[17] *Id.* at 1328.

Pending Actions

Wendy's

In December 2016, a plaintiff shareholder filed a derivative suit in the Southern District of Ohio against Wendy's and certain directors and officers related to a data breach that compromised customers' personal and financial information.[18] The breach occurred from October 2015 through June 2016 and affected the point-of-sale systems of over 1,000 Wendy's franchise locations.

The plaintiffs asserted claims for breach of fiduciary duty, waste of corporate assets, unjust enrichment, and gross mismanagement. The plaintiffs sought not only damages but also corporate governance reforms and restitution of benefits and compensation from the director and officer defendants.

The complaints specifically allege that the directors and officers failed to implement and enforce effective data security internal controls and procedures, failed to oversee and monitor compliance with various laws and regulations, failed to cause the company to make full disclosures concerning, among other things, the scope and impact of the breach, and permitted the company to violate industry data security standards.

On March 10, 2017, the defendants moved to dismiss the complaint for failure to state a claim and for failure to make a demand or adequately plead demand futility. The plaintiff claims that demand was futile because the current director defendants face a substantial likelihood of liability and have deep-rooted relationships with each other such that they are incapable of making an independent and disinterested decision regarding whether to pursue legal action.

The court has yet to rule on the defendants' motion to dismiss. Following the filing of the motion, another plaintiff shareholder filed a new derivate suit alleging overlapping claims. While the motion to appoint lead plaintiff was pending, a proposed stipulation of settlement was filed between the defendants and one of the two plaintiffs, which is still pending approval by the court. Thus, it remains to be seen whether the plaintiff can overcome the incredibly stringent standards of demand futility and whether any data breach–related derivative suit is capable of proceeding past the motion to dismiss phase.

Yahoo

In February 2017, Yahoo! Inc. ("Yahoo") shareholders filed a derivative suit in Delaware Chancery Court alleging that the company breached its fiduciary duties by failing to disclose for over two years security breaches in which the personal information of over 1.5 billion user accounts was stolen.[19] The plaintiffs allege that Yahoo only disclosed the security breaches after Verizon, to whom Yahoo had agreed to sell its web business, questioned the company about rumors of a hack.[20]

According to the complaint, in concealing the breaches, the directors and officers not only damaged Yahoo's reputation but also subjected the company to significantly greater liability, including in consumer class action lawsuits and adverse regulatory actions, and caused the company to make misrepresentations to its users, stockholders, and Verizon. Further, the plaintiffs allege that the concealment of the breaches caused Verizon to delay the acquisition of Yahoo, as well as to seek a discount on the deal.

The plaintiffs did not make a pre-suit demand on the board, but rather allege that such a demand would be futile, as the directors lack the requisite independence to determine whether the claims should be pursued.

Derivative suits involving similar claims and allegations are also currently pending in the Superior

[18] Verified Shareholder Derivative Complaint, *Graham v. Peltz*, No. 16-CV-1153 (S.D. Ohio Dec. 16, 2016).

[19] Verified Derivative Complaint, *Okla. Firefighters Pension & Ret. Sys. v. Brandt*, No. 2017-0133-SG (Del. Ch. Feb. 23, 2017). A securities class action complaint, described below, was filed against Yahoo regarding the same breaches, and alleges that hackers stole the records of over three billion users. Second Amended Complaint ¶ 2, *In re Yahoo! Inc. Sec. Litig.*, No. 17-cv-00373-LHK (N.D. Cal. Feb. 2, 2018).

[20] Verified Derivative Complaint ¶¶ 19-20, *Okla. Firefighters Pension & Ret. Sys. v. Brandt*, No. 2017-0133-SG.

Court of the State of California County of Santa Clara.[21]

Lessons Learned

More than anything, the shareholder derivative suits filed in the wake of cybersecurity breaches demonstrate the hurdles that plaintiffs face in overcoming the business judgment rule and pre-suit demand requirement. Nevertheless, courts have made clear that directors and officers must respond in *some* reasonable way to the real threat of cybersecurity breaches. It is not only important that companies consider implementing robust preventive security measures that are in compliance with industry standards, but it is also vital that companies move swiftly in the wake of a breach to minimize damage, and accurately and timely make disclosure of the incident to those affected (including shareholders).

Securities Fraud Class Actions

Settled Actions

ChoicePoint

In March 2005, in one of the earliest data-breach securities class actions, a federal securities class action was filed against ChoicePoint, a data collection company that provided identification and credential verification services. Plaintiffs brought claims under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act"), and Rule 10b-5 promulgated thereunder, alleging that the company and certain officers and directors concealed and misrepresented the existence and severity of data and privacy security problems, causing the company's stock to be artificially inflated.[22] In September 2004, ChoicePoint learned that for over a year, one of its customers had illegitimately accessed highly sensitive records of tens of thousands of ChoicePoint's customers and had been selling the information to criminals.[23] Plaintiffs alleged that, prior to the breach, ChoicePoint failed to improve its data security, despite repeated warnings from its employees about the risk of a potential breach, as well as in the face of previous data breaches.[24]

The Northern District of Georgia denied defendant's motion to dismiss on November 21, 2006, but pursuant to previous more lenient pleading standards under *Conley v. Gibson*, 355 U.S. 41 (1957).[25] The court rejected, among other arguments, defendants' contention that the alleged misleading statements touting the company's privacy protections were ones of general corporate optimism or puffery.[26] It reasoned that defendants' knowledge of previous security breaches and inadequate security procedures rendered the statements material and elevated them above the realm of puffery.[27] The court also held that plaintiffs adequately alleged scienter where the defendants had access to internal information demonstrating the falsity of the public statements and where suspicious insider trading had occurred.[28]

The parties ultimately settled the action for $10 million in March 2008.[29] The court approved the parties' settlement agreement on July 21, 2008, deeming the settlement fair, reasonable, and adequate, in part because plaintiffs' success at trial was far from assured, given anticipated difficulties in proving materiality, scienter, and loss causation.[30]

[21] *In re Yahoo! Inc., Shareholder Litig.*, No. 17-CV-307054 (Cal. Super. Ct. Santa Clara Cnty.) (docket).

[22] Amended Complaint, *In re ChoicePoint, Inc. Sec. Litig.*, No. 05-CV-00686-JTC (N.D. Ga. Jan. 13, 2006).

[23] *Id.* ¶¶ 4, 58-62, 101.

[24] *Id.* ¶¶ 52-56.

[25] Defendants filed a motion for reconsideration in June 2007, after the Supreme Court issued its decision in *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007). The parties, however, settled the action before the court rendered a decision on the motion.

[26] Order Denying Motion to Dismiss at 15-16, *In re ChoicePoint, Inc. Sec. Litig.*, No 05-CV-00686-JTC (N.D. Ga. Nov. 21, 2006).

[27] *Id.*

[28] *Id.* at 19-20.

[29] Stipulation of Settlement, *In re ChoicePoint, Inc. Sec. Litig.*, No. 05-CV-00686-JTC (N.D. Ga. Mar. 7, 2008).

[30] Findings of Fact and Conclusions of Law Concerning Motion for Final Approval of Class Action Settlement at 6-9, *In re*

Dismissed Actions

Heartland

In December 2009, the District Court of New Jersey dismissed a securities fraud action against Heartland Payment Systems, Inc. ("Heartland"), a payment processing service provider, regarding alleged misstatements and omissions in connection with a 2007-2008 cyberattack that resulted in the theft of 130 million credit card and debit card numbers.[31] Defendants initially believed that the incident only targeted an internal system and that the hackers failed to steal any information, and therefore did not immediately disclose the attack. When it discovered the true extent of the breach in 2009, it swiftly disclosed the theft. Plaintiffs brought claims under Sections 10(b) and 20(a) of the Exchange Act, and Rule 10b-5 promulgated thereunder, alleging that defendants fraudulently concealed the attack and misrepresented the general state of data security at Heartland.

In dismissing the action, the court held that plaintiffs failed to identify any material misstatements or omissions and failed to adequately allege scienter.[32] It explained that Heartland's statements that it placed "significant emphasis on maintaining a high level of security" were not inconsistent with the fact that the company had suffered an attack—the fact that a company faces security problems does not necessarily suggest that it does not value data security.[33] The court also pointed to certain cautionary statements the company made, which warned of the possibility of a breach, to show that Heartland never claimed its security system was invulnerable.[34] With respect to certain alleged omissions, the court found that general affirmative statements about network security do not necessarily give rise to a duty to disclose related facts regarding data breaches.[35] Finally, the court held that plaintiffs failed to allege facts sufficient to support an inference that defendants knew that Heartland was not paying proper attention to its security problems.[36] The court did not reach the issue of loss causation.

The court's decision highlights the difficulties of succeeding on securities fraud claims based on a theory of alleged omissions. The court acknowledged that had plaintiffs known about the initial attack, they might not have purchased Heartland securities, but dismissed the action nevertheless because there is no general duty to disclose every material fact. The decision also demonstrates the importance of robust and targeted risk disclosures, which in certain situations may foreclose liability in the face of a breach.

Pending Actions

Yahoo

In January 2017, investors filed a securities class action pursuant to Sections 10(b) and 20(a) of the Exchange Act, and Rule 10b-5 promulgated thereunder, against Yahoo regarding alleged misstatements and omissions in connection with the same data security breaches that were the subject of the shareholder derivative suit described above. Plaintiffs allege that defendants failed to disclose "the two largest data breaches in U.S. history," in which hackers stole the records of over three billion users,[37] despite Yahoo's contemporaneous knowledge of the breaches. Further, plaintiffs allege that defendants fraudulently reassured the public that Yahoo employed best practices in safeguarding personal information, even though it used grossly outdated security systems. When the market learned of the data breaches, Yahoo's shares dropped by over 31%, according to plaintiffs.[38]

ChoicePoint, Inc. Sec. Litig., No. 05-CV-00686-JTC (N.D. Ga. July 27, 2008).

[31] Amended Complaint ¶ 5., *In re Heartland Payment Systems, Inc. Sec. Litig.*, No. 09-CV-01043-AET-TJB (D.N.J. Aug. 20, 2009).

[32] *In re Heartland Payment Sys., Inc. Sec. Litig.*, No. 09-CV-01043-AET-TJB, 2009 WL 4798148 (D.N.J. Dec. 7, 2009).

[33] *Id.* at *5.

[34] *Id.*

[35] *Id.* at *6-7.

[36] *Id.* at *7-8.

[37] Second Amended Complaint ¶ 2, *In re Yahoo! Inc. Sec. Litig.*, No. 17-cv-00373-LHK (N.D. Cal. Feb. 2, 2018).

[38] *Id.* ¶ 7.

In July 2017, Yahoo moved to dismiss the complaint, arguing that plaintiffs failed to plead falsity, scienter, and loss causation or damage. Citing the decision in *In re Heartland* described above, Yahoo explained that the fact that the company was the victim of a security breach does not render its statements concerning its aspirational commitments to user privacy misleading, which in any event were mere unverifiable expressions of optimism that do not give rise to a securities claim.[39] Defendants argued that they warned of the uncertainty of the success of their security efforts and that these risk warnings do not trigger a duty to disclose more.

On November 22, 2017, the court provided plaintiffs with leave to amend their First Amended Complaint, in light of Yahoo's October 3, 2017 disclosure that the 2013 data breach affected an additional two billion Yahoo user accounts. The court thus denied, without prejudice, the motion to dismiss as moot.

On March 2, 2018, the parties entered into a stipulation and agreement of settlement, and on May 9, the court granted an order of preliminary approval.[40] Given the settlement, it is unlikely that this case will provide a vehicle for the court to clarify the contours of a defendants' duty to disclose in the cybersecurity context.

Equifax

On September 8, 2017, investors filed a securities class action against Equifax, a consumer credit reporting company, just one day after it disclosed a massive cybersecurity incident that potentially impacted 143 million U.S. consumers.[41] Plaintiffs, who bring claims under Sections 10(b) and 20(a) of the Exchange Act, and Rule 10b-5 promulgated thereunder, allege that Equifax's failure to maintain adequate measures and monitoring systems to protect against and detect security breaches render its public statements regarding its data security materially misleading. Plaintiffs also allege that after the breach was discovered, but before Equifax disclosed it, the company's CFO and two other executive officers sold a portion of their shares, providing support that defendants acted with scienter. While the security breach occurred from mid-May through July 2017, Equifax only announced the incident in early September 2017. On release of the news, plaintiffs allege that Equifax's share price dropped significantly.

In comparison to other securities lawsuits following data breaches, the action against Equifax appears more promising for plaintiffs given the scale of the incident, the extent of the price drop, and the allegations of insider trading that may support an inference of scienter.

PayPal

Investors filed a securities class action on December 6, 2017, against PayPal, an online payment platform, just six days after the company disclosed a data breach in connection with its recent acquisition of the bill-pay management company, TIO Networks Corp. ("TIO").[42] On November 1, 2017, PayPal suspended its TIO services, stating that it had discovered certain security vulnerabilities. One month later, on December 1, PayPal disclosed that personally identifiable information for about 1.6 million TIO users had potentially been compromised. Plaintiffs allege that on this news, PayPal's share price declined 5.75%.

Plaintiffs, who bring claims under Sections 10(b) and 20(a) of the Exchange Act, and Rule 10b-5 promulgated thereunder, allege that defendants made misleading statements or omissions regarding the adequacy of TIO's data security program and had thus overstated the benefits of the TIO acquisition.

Notably, plaintiffs provide sparse allegations with respect to scienter—they merely allege in a conclusory way that defendants had actual knowledge of the

[39] Motion to Dismiss at 7, *In re Yahoo! Inc. Sec. Litig.*, No. 17-cv-00373-LHK (N.D. Cal. July 28, 2017).

[40] Order Granting Motion for Preliminary Approval of Settlement, *In re Yahoo! Inc. Sec. Litig.*, No. 17-cv-00373-LHK (N.D. Cal. May 9, 2018).

[41] Complaint, *In re Equifax Inc. Sec. Litig.*, No. 17-CV-03463-TWT (N.D. Ga. Sept. 8, 2017).

[42] Complaint, *Sgarlata v. PayPal Holdings, Inc.*, No. 17-cv-06956-EMC (N.D. Cal. Dec. 6, 2017).

misstatements and omissions and intended to deceive plaintiffs. It remains to be seen what specific theories plaintiffs will advance to show defendants' scienter, especially in light of PayPal's apparent timely and transparent response to the security threat.

Qudian

On December 12, 2017, plaintiffs brought a securities class action against Qudian, a Chinese online microlender, alleging violations of Sections 11 and 15 of the Securities Act of 1933 (the "Securities Act").[43] Plaintiffs allege that there were material misrepresentations or omissions in the company's offering documents in connection with its recent IPO, because Quidan failed to disclose that it had experienced data breaches and that its data systems and procedures were materially inadequate to protect sensitive borrower data.[44] The complaint also focuses on claims unrelated to its data protections, including omissions regarding the deficiency of Quidan's loan collection practices.

While plaintiffs allege a stock decline of 45%,[45] they may face difficulties in attributing the decline to the data breach. At the same time that news of the data breach began circulating, the Chinese government initiated a crackdown on payday loans.[46]

Lessons Learned

There has been a clear recent uptick in securities class actions following a number of data breaches. While few such cases were filed prior to 2017, four cybersecurity-related securities lawsuits were brought in just the last year. It remains to be seen whether these suits will be successful, but it is an important reminder that companies should make data security a key priority.

These recent cases demonstrate that, in the aftermath of a breach, investors tend to seize on statements the company previously made regarding the effectiveness of its privacy and data security regime. Thus, companies should carefully review any disclosures it makes or has made regarding data security to ensure that they are accurate and necessary. Companies should also carefully consider the SEC's new cybersecurity disclosure guidance that was released in February 2018.

Further, investors tend to focus on inadequate responses to data breaches or the failure to immediately disclose cyber incidents. Companies should enhance their monitoring mechanisms to better detect breaches and should also prepare response plans in advance of any security breach, which should set forth all of its reporting obligations.

While cyberattacks have become nearly inevitable, there are a number of steps that companies can take, both before and after an incident, to prevent or minimize securities liability. The success or failure of this recent wave of securities class actions will undoubtedly provide further lessons for companies trying to reduce and manage the risk of such suits.

[43] Complaint, *Ramnath v. Qudian Inc.*, No. 17-cv-9741 (S.D.N.Y. Dec. 12, 2017).

[44] *Id.* ¶ 35.

[45] *Id.* ¶ 37.

[46] Kevin LaCroix, *Yet Another Data Breach-Related Securities Suit Filed*, The D&O Diary (Dec. 13, 2017), https://www.dandodiary.com/2017/12/articles/securities-litigation/yet-another-data-breach-related-securities-suit-filed/.