The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 2 January 31, 2018

BOARDS OF DIRECTORS

# Dynamic Regulations and Shareholder Actions Guide the Board's Shifting Role in Cyber (Part One of Two)

By Jeewon Kim Serrato, Marc Elzweig, David Lee
Shearman & Sterling

One well-known cost of breaches is post-breach litigation. A growing trend that merits further attention is the rise of shareholder derivative suits filed against boards of directors of companies that suffered data breaches. Moreover, regulatory changes, including the GDPR, may make such suits more frequent in addition to creating other data-breach-response expenses. Boards of directors need to take note and understand these increasing costs and risks.

In part one of this two-part article series, we review the evolving understanding of the board of directors' responsibility for cybersecurity and consider several shareholder derivative suits filed in the wake of data breaches as case studies. In part two, we will consider some of the lessons that boards may learn from these suits.

### *Rising Costs and Regulatory Shifts*

Not only are data breaches expensive in direct costs, but they may also have a persistent or permanent negative impact. A recent CGI and Oxford Economics study found an average permanent loss of nearly 2% of a company's value resulting from a severe data breach, and that the impact is likely increasing. In addition, data breach reporting requirements in the E.U. GDPR are reasonably expected to increase the global reporting of and scrutiny on data breaches after the GDPR becomes effective on May 25, 2018. We may learn that data breaches are even more common and expensive than our current understanding.

Consumer class actions typically follow a breach, and there may be litigation with other third parties, such as credit card processers if payment card systems are compromised. Such suits often lead to significant expenses for the company, and the impact of consumer class actions and suits filed by financial institutions have received wide coverage.

In addition to class actions, in several recent large-scale data breach incidents, shareholders have filed suits against the executives and directors for various theories including breach of fiduciary duties, mismanagement and material omissions.

With the GDPR on the one hand mandating data breach notifications and on the other explicitly allowing for private claims and group action claims – where individuals may mandate a not-for-profit body, organization or association to exercise their rights and bring claims on their behalf – we expect to see an increased awareness of data breaches and resulting claims against companies.

See "Key Post-Breach Shareholder Litigation, Disclosure and Insurance Selection Considerations" (Aug. 3, 2016).

### *Board Considerations*

Increased regulatory obligations, alongside media reporting on data breaches that have led to the ouster of CEOs and shakeups of boards, have made cybersecurity threats a top concern for boards of directors. The new GDPR breach notification rules and the specter of fines and private claims will also dramatically increase the need for board oversight in handling E.U. resident data. Shearman & Sterling's 2017 Corporate Governance & Executive Compensation Survey, an annual survey of the 100 largest U.S. public companies, showed that 15% of the companies' shareholder engagement disclosures in their 2017 proxy statements included risk management and oversight, cybersecurity and compliance issues, compared to 7% in 2016.

An increase in knowledge and awareness of cybersecurity issues may be prompting more disclosures. The 2017 BDO Cyber Governance Survey reports that more than three-quarters (79%) of public company directors report their board is more involved with cybersecurity than it was 12 months ago. Given the exposure, we anticipate more companies will add cybersecurity statements in their proxy statements.

See "A CSO/GC Advises on How and When to Present Cybersecurity to the Board" (Feb. 22, 2017).

The following are some of the notable regulatory developments – through the GDPR and U.S. regulatory efforts – that boards should keep in mind.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Vol. 4, No. 2 January 31, 2018

### *GDPR's Breach Notification Provision*

In the E.U., the GDPR is slated to be one of the most significant pieces of legislation in decades and presents ambitious and comprehensive changes to data protection rules that will surely be tested in court. Intended to harmonize E.U. member state legislations and increase data subjects' rights, the GDPR not only requires companies handling E.U. resident data to comply with privacy principles, but it also includes the first E.U.-wide mandatory data breach notification rule. Under Article 33, companies are required to report to the data protection supervisory authority within 72 hours all breaches leading to destruction, loss, alteration or unauthorized access to personal data that is likely to result in a risk to the rights and freedoms of the affected data subjects. Further, under Article 34, when a data breach is likely to result in a "high risk" to the rights and freedoms of natural persons, notification to data subjects is required without undue delay.

See "A Practical Look at the GDPR's Data Breach Notification Provision" (Jan. 17, 2018).

### *GDPR's Right of Compensation*

In addition to this mandatory breach notification rule, which is similar to rules the U.S. has had for over a decade,[1] the GDPR also gives individuals a right to compensation from a data breach. Under Article 79, individuals may bring private claims for any infringement of the GDPR relating to the processing of their personal data. Article 82(1) expands the scope of liability for infringement so that anyone who has suffered material or non-material damage shall have the right to compensation.

It is important to note that the injured person no longer needs to prove financial loss to recover from the lawsuit, as damages may be awarded to a person who suffered distress due to the breach. The GDPR also allows third party not-for-profit public interest bodies to bring claims on data subjects' behalf (Article 80(1)). These new rules significantly expand the pool of claimants who may seek damages against a company in the case of a data breach.

Not only will data breaches result in private claims, failures to comply with the GDPR can result in fines of up to 4% of global revenue. As a result, this legislation will likely place cybersecurity and personal data issues at the top of the board agenda.

See "A Discussion With Ireland's Data Protection Commissioner Helen Dixon About GDPR Compliance Strategies (Part One of Two)" (Mar. 22, 2017); Part Two (Apr. 5, 2017).

### *U.S. Regulators' Views on Board Behavior*

In the U.S., there is no national data protection or cybersecurity law, but a patchwork of state and federal regulations have sought to address cybersecurity threats and privacy issues, with regulators increasingly signaling that the board has oversight responsibilities. In a 2014 speech to the New York Stock Exchange, then-SEC Commissioner Luis Aguilar noted that "boards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. … and there can be little doubt that cyber-risk also must be considered as part of boards' overall risk oversight."

Similarly, Jay Clayton, during 2017 confirmation hearings to become Chairman of the SEC, signaled his support for a Senate bill that would increase disclosure about directors' roles and expertise in cybersecurity. Mr. Clayton stated, "I believe that is something that investors should know, whether companies have thought about the [cybersecurity] issue, whether it's a particular expertise the board has," and further added, "It's a very important part of operating a significant company." These statements reflect the SEC's position that "the greatest threat to our markets right now is the cyber threat," as stated by Steven Peikin, SEC's co-director of enforcement.

See also "SEC Officials Flesh Out Cybersecurity Enforcement and Examination Priorities (Part One of Two)" (May 3, 2017); Part Two (May 17, 2017).

### *State and Regulatory Guidance*

In an effort to address these threats for the financial sector, the Federal Deposit Insurance Corporate, the Federal Reserve and the Comptroller of the Currency issued a joint advance notice of proposed rulemaking (ANPR) in 2016 regarding enhanced cyber risk management standards. After receiving comments from the industry, however, regulators decided not to move forward with the final rule. In the meantime, the National Association of Insurance Commissioners (NAIC) adopted the Insurance Data Security Model Law, which creates uniform rules for insurers, brokers, agents, and other licensed entities regarding data security, investigation and data breach.

At the state level, the New York State Department of Financial Services (NYDFS) put into effect the Cybersecurity Requirements for Financial Services Companies in August 2017, including specific provisions to ensure that boards take responsibility for cybersecurity. In addition to requiring a cybersecurity program and written policies, the regulations require each entity to designate a CISO who must submit reports to the board at least annually to inform the board of the entity's cybersecurity program and risks. The regulations also require that the board, an appropriate board committee or a senior officer, annually approve the entity's cybersecurity policy and file a certification of compliance. Further, in comments to the regulations, NYDFS stressed that "a well-informed board is a crucial part of an effective cybersecurity program and the CISO's reporting to the full board is important to enable the board to assess the [entity's] governance." The first such certifications of compliance are due February 15, 2018.

See also "What Covered Financial Entities Need to Know About New York's New Cybersecurity Regulations" (Mar. 8, 2017).

### *More to Come*

This NYDFS cyber regulation was the first of its kind in the U.S., and other U.S. states are likely to follow. Colorado, for example, recently passed cybersecurity rules for broker-dealers and investment advisers subject to the Colorado Securities Act. Even without a national cybersecurity risk management standard, there are numerous rules and regulations that firms must follow for cybersecurity compliance. Kevin Gronberg, vice president of JP Morgan Chase global cyber partnerships, has commented that a collection of all U.S. and global guidance documents, regulatory requirements and recent proposals on cybersecurity impacting the financial sector resulted in a 2,000-line spreadsheet.

See "How In-House Counsel, Management and the Board Can Collaborate to Manage Cyber Risks and Liability (Part One of Two)" (Jan. 20, 2016); Part Two (Feb. 3, 2016).

## *Examining Recent Shareholder Suits*

Although there is currently only a limited set of cases, it is worth considering these examples of shareholder derivative suits filed after a data breach. In general, shareholder derivative suits filed in the U.S. in response to data breach incidents generally face two significant hurdles to survive a motion for dismissal: the business judgement rule and the demand futility requirement. The cases below demonstrate the difficulties posed by these two hurdles and how they may influence the outcomes and impacts of such cases.

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

### *The TJX Companies Case*

One of the first major shareholder derivative suits filed in response to data breach was against TJX Companies Inc., the retail company whose stores include T.J. Maxx and Marshalls. Beginning in July 2005, hackers infiltrated TJX systems, installed sniffers to capture the company's network traffic and copied stored data. The intrusion continued until January 2007 and resulted in the theft of at least 45.7 million credit and debit card records. At the time, it was considered the largest data breach incident ever, effectively rewriting ideas of scale for modern data breach incidents.

In 2010, the Louisiana Municipal Police Employees' Retirement System filed a shareholder derivative suit against the directors of TJX, alleging that the TJX directors breached their fiduciary duty by failing to adequately prepare for a cybersecurity attack. The plaintiff alleged that the directors breached their duty of loyalty, care and good faith by failing to comply with Payment Card Industry Data Security Standards (PCI DSS) and best practices by lacking effective firewalls and sufficient wireless encryption, and by storing payment card data in clear text.

The case settled 13 days after the complaint was filed and did not reach the merits. The settlement required TJX to set up a toll-free number to handle questions relating to the data breach. In addition, the audit committee would oversee cybersecurity issues and make reports to the board, with access for plaintiff's counsel to provide suggestions to prevent future incidents, and internal policies would be updated to reflect the new oversight roles.

### *The Wyndham Case*

Between 2008 and 2010, Wyndham Worldwide Corporation's hotels suffered three distinct data breaches, resulting in unauthorized access to more than 600,000 customer records,

including payment card information. These data breaches resulted in an FTC complaint filed against the company in 2012.

Following the FTC complaint, shareholder Dennis Palkon sent a letter to the Wyndham board demanding that it investigate and remedy the harm inflicted on the company through the data breaches, which the board voted unanimously not to pursue, resulting in a 2014 shareholder derivative suit filed against the company. The plaintiff alleged breach of fiduciary duties and of audit responsibilities and described egregious cybersecurity failures, including lack of firewalls, use of computer systems so out of date that they no longer received security patches, customer data and credit card information stored in plain text, and a failure to address these issues even after the company became aware of intrusions into its computer systems.

Despite these allegations, the case was dismissed under the business judgment rule. Under Delaware law, the board's decision not to pursue the shareholder's demand letter falls within business judgement rule, where the court presumes that the board's refusal was informed, made in good faith, and taken in the honest belief that it is in the best interest of the company. The court found that the plaintiff's allegations failed to rebut the presumption by raising a reasonable doubt that the board acted in good faith or based on a reasonable investigation. In reaching this conclusion, the court noted that Wyndham's board and audit committee discussed the breaches and the demand letter at numerous meetings, and that the board's understanding of the issues also developed in context of the FTC investigation.

The Wyndham case demonstrates the high bar that a plaintiff faces in a shareholder derivative suit. Although it is not clear how similar circumstances would be viewed under the present understanding of the importance of cybersecurity and board responsibilities, Wyndham still demonstrates the legal protections around a board's actions in response to a data breach and resulting demand letter.

See "In the Wyndham Case, the Third Circuit Gives the FTC a Green Light to Regulate Cybersecurity Practices" (Aug. 26, 2015).

### *The Target Case*

Hackers gained access to Target's computer systems in 2013 and installed malware on its point-of-sale systems, which remained from November 27 to December 25. While the malware stole credit card information of approximately 40 million customers, the hackers stole personal information records of another 70 million customers. At the time, the Target attack constituted one of the largest breaches of consumer data in the U.S.

The following month, in January 2014, two shareholder derivative suits (here and here) were filed against Target. Plaintiffs in each suit alleged that executives and directors breached fiduciary and other duties, and recklessly disregarded their duties, based on failures to securely maintain customer data, or to implement internal controls to detect and prevent a data breach. Neither plaintiff made a litigation demand to the board, arguing that such a demand would be futile.

Both suits were ultimately dismissed, but Target followed a different path to dismissal. In response to a litigation demand received by the board before either suit was filed, Target's board established a special litigation committee (SLC) consisting of two newly-appointed independent directors with separate legal counsel. The SLC conducted a two-year investigation into the data breach to determine whether executives and directors conduct violated their fiduciary duties, including review of thousands of documents and 68 witness interviews. In 2016, the SLC produced a lengthy report detailing Target's security practices prior to the data breach and changes to its security measures implemented after the event, and determining that it was not in Target's best interest to pursue litigation. When the special litigation committee sought dismissal of the suits, plaintiffs did not oppose, and both suits were dismissed.

See "Takeaways From State AGs' Record-Breaking Target Data Breach Settlement" (May 31, 2017).

### *The Home Depot Case*

Home Depot's cash register systems were compromised from April 2014 to September 2014, resulting in the theft of 56 million cardholders' information. In the first resulting derivative suit, the plaintiffs alleged that Home Depot's officers and directors breached their fiduciary duties by failing to ensure that the company implemented reasonable measures to protect customers' information, including by the company's failure to comply with PCI DSS standards. The complaint also alleges that the company had knowledge and warnings of its insufficient security measures. In addition, the

plaintiffs alleged corporate waste and violation of Section 14(a) of the Securities Exchange Act. Plaintiffs did not make a demand to the board and argued that a demand would be futile.

In November 2016, the district court dismissed the derivative suits under the demand futility standard. Under Delaware law, a shareholder is required to make a demand to the board, to seek desired actions, prior to filing a shareholder derivative suit. A plaintiff may argue that a demand would be futile, but in cases based on inaction of the board, the plaintiff must show by particularized factual allegations that at the time of filing there was a reasonable doubt that the directors could properly exercise independent and disinterested business judgment in responding to a demand.

In analyzing the plaintiffs' duty of loyalty claims, the court noted that when the proof of failure of oversight requirement is added to the general demand futility requirement, the plaintiff must show with particularized facts and beyond a reasonable doubt that a majority of the board faced substantial liability because it consciously failed despite a known duty. The court described this as "an incredibly high hurdle for the Plaintiffs to overcome" and found the plaintiffs failed to do so, in part because plaintiffs acknowledged that the board took action to address security weaknesses before the breach occurred.

The court similarly applied the demand futility requirement to the plaintiffs' corporate waste and Section 14(a) claims and found plaintiffs failed to demonstrate the futility of demands for those claims as well.

The Home Depot case demonstrates the high hurdles for a shareholder derivative suit to survive dismissal. The case acts potentially as precedent for the data breach derivative suits to follow, but it is also notable for what happened after dismissal. Plaintiffs filed an appeal of the dismissal, and the parties subsequently settled in April 2017. The settlement provides up to $1.125 million in attorneys' fees and requires various reforms of the company's data security policies and controls. Similar to the TJX case, there was no "victory" for plaintiffs in court. However, the cases still demonstrate how shareholder derivative suits following data breaches, despite their high burdens on plaintiffs, may result in significant legal costs and settlements.

Settlement of the Home Depot case will likely become additional fuel for future shareholder derivative suits. Currently, there is at least one pending shareholder derivative suit based on a data breach, filed against Wendy's Co. in December 2016. It is expected that more of these cases will follow, such as in the Equifax data breach and large data breaches that appear inevitable in 2018.

See "Protecting Attorney-Client Privilege and Attorney Work Product While Cooperating With the Government: Implications for Collateral Litigation (Part Three of Three)" (Mar. 8, 2017).

*Jeewon Kim Serrato is counsel at Shearman & Sterling and head of the privacy & data protection group. She advises companies on privacy, cybersecurity, data protection and crisis management issues. She has extensive experience in developing and structuring comprehensive data and trade secrets protection programs, implementing and testing information security controls, and helping companies mitigate cyber risks and handle data breaches. Previously, she served as chief privacy officer of Fannie Mae. She also currently serves on the Department of Homeland Security Data Privacy and Integrity Advisory Committee Technology Subcommittee.*

*Marc Elzweig is an associate in the Privacy & Data Protection and IP Transactions practice groups at Shearman & Sterling.*

*David Lee is an associate in the Privacy & Data Protection group at Shearman & Sterling.*

[1] The first such law, the California data security breach notification law was enacted in 2002 and became effective on July 1, 2003. See SB 1386, Cal. Civ. Code 1798.82 and 1798.29