2020 Annual Conference
March 18-20, 2020
Dallas, TX

Trending Headlines or Fake News? Potential D&O Exposures to Watch in 2020 Including Cyber Risks

Significant potential exposures to corporations, their directors and officers, and their directors and officers (D&O) insurers continue to exist in the historical and familiar types of claims, although sometimes with a new twist—securities litigation with increasing numbers of state court actions, derivative actions without stock drops and with nine figure settlements, more government investigations and enforcement actions. There is also continued fallout from opioid, sexual misconduct, and other event-driven litigation. Emerging issues such as evolving cyber risks are among the topics high on the list of concerns of corporate boards and their insurers. In addition to potential coverage under D&O policies for cyber risks, boards and their brokers are also looking to cyber and other categories of policies for coverage options for data breaches, privacy violations, malware attacks and the increased threat of direct personal liability to corporate executives. All of these potential risks in addition to the ever-increasing costs of litigation continue to increase exposures to corporations and their management as well as their insurers.

I. D&O Exposures—Current Trends and Issues

A. Securities Class Actions

1. Number of Filings

In 2018, securities lawsuit filings reached their highest level since 2001. (*See*, Boettrich & Starykh, "Recent Trends in Securities Class Action Litigation: 2018 Full-Year Review," www.nera.com.) Although filings had been relatively stable since 2007, new filings have doubled since 2014 when there were 218 federal court securities class action filings. That number grew in 2017 to 434 and was slightly higher again in 2018 at 441 new filings. In 2019, there were 341 federal court securities lawsuit filings between January and September indicating a continued upward trend. (*See*, Starykh & McIntosh, "Recent Trends in Securities Class Action Litigation: 2019 Q3 Update," www.nera.com.)

While the increased number of filings may be reflective of some different types of cases, the number of more standard securities class action lawsuits such as those resulting from financial

misstatements or accounting misrepresentations are also above historical levels. Of the 341 securities class actions filed between January and September 2019, 204 were traditional lawsuits alleging violations of U.S. securities laws. This figure suggests a trend to a year-end total of 272 standard securities lawsuits, which is, by historical standards, an extraordinary number of securities lawsuit filings and would be higher than the annual total number of securities lawsuit filings in any year during the period 2003 to 2015.

2. *Cyan* Impact

Although there has been a significant growth in the number of federal court filings, these numbers do not fully reflect the actual increase in securities class action litigation. The number of state court filings has also increased significantly in the wake of the U.S. Supreme Court's *Cyan* decision, in which the court held that state courts retain concurrent jurisdiction for cases involving alleged violations of the 1933 Securities Act. *Cyan, Inc. v. Beaver Cty. Emps. Retirement Fund*, 138 S. Ct. 1061 (2018). More Securities Act claims were filed in New York state courts in the first half of 2019 than in California making New York the focus of a significant portion of state court securities litigation. *See*, Cornerstone Research, "Securities Class Action Filings Mid-Year Assessment," www.cornerstone.com.

The havoc created by *Cyan* has been well-documented in the D&O press. (*See, e.g.,* LaCroix, "Multiplied and Parallel Litigation: The Mess that Cyan has Wrought," *The D&O Diary*, Nov. 18, 2019.) Until this issue is addressed by Congress, there are likely to be many inconsistent rulings given the number of courts that are addressing claims under the Securities Act for the first time. In the Eastern District of Tennessee, a federal judge recently ruled that *Cyan* required the remand of previously removed state court securities actions. *Gaynor v. Miller*, No. 3:15-cv-545, E.D. TN (Dec. 6, 2019). Meanwhile, state courts are learning about securities law with mixed results. From the state courts of New York, there have been several rulings in post-*Cyan* cases in 2019. *See, In re Netshoes Securities Litigation*, 2019 WL 3227251, (Sup. Ct. N.Y. Cty. July 16, 2019); *In re PPDAI Group Securities Litigation*, 2019 WL 2902150, (Sup. Ct. N.Y. Cty. July 5, 2019); *Hoffman v. AT&T Inc.*, 2019 WL 2578360, (Sup. Ct. N.Y. Cty. June 21, 2019). In other states, including Connecticut and Texas, state court judges have allowed securities class actions to proceed but then granted the defendants' motions to dismiss based on a substantive analysis of the law. *See, e.g. City of Livonia Retiree Health and Disability Benefits Plan et al. v. Pitney Bowes Inc. et al.,* No. X08-FST-CV-18-6038160-S, CT Superior Court (Oct. 24, 2019)

3. Merger-Objection Litigation

The number of merger-objection lawsuits continues to increase. These lawsuits typically allege that the company's board of directors breached its fiduciary duties by conducting a flawed sale process that failed to maximize shareholder value. In 2009, there were 24 merger-objection filings in the 205 securities class action lawsuits filed. By 2016, the number had grown to 92. In 2017, merger-objection filings jumped to 204 and were relatively stable in 2018 at 210 filings. The rate of merger-objection lawsuits has also increased. In 2018, 82% of mergers were met with litigation objecting to the merger and nearly 1 in 10 S&P 500 companies was the target of a merger-objection lawsuit. *See*, LaCroix, "Percentage of 2018 Deals Drawing Merger Objection Suits Held Steady," *The D&O Diary*, (Sept. 17, 2019).

Merger-objection lawsuits are frequently resolved by "disclosure-only" settlements in which plaintiffs' counsel receive a payment of fees and shareholders get a "supplemental disclosure" of information not included in the original proxy statement for the proposed merger. Disclosure-only settlements may result in minimal or no monetary recovery for shareholders but they are still expensive and the costs to defend and settle these cases are increasing. One insurer has reported that its average costs associated with a settled merger-objection lawsuit increased 63% between 2012 and 2016, from $2.8 million to $4.5 million. Payments to shareholders during this period were 39% of the total with 61% of costs paid to plaintiffs and defense counsel for attorney fees and expenses. See, Chubb Press Release, "Rising Volume and Costs of Securities Class Action Lawsuits is Growing Tax on U.S. Business, Chubb Data Reveals," www.news.chubb.com, (July 10, 2018).

Courts have begun to more aggressively scrutinize disclosure-only settlements. In *In re Trulia, Inc. Stockholder Litigation,* the Delaware Court of Chancery rejected one such settlement, finding that the supplemental disclosures were not "material or even helpful" to shareholders. *In re Trulia*, 129 A.3d 884 (Del. Ch. 2016). More recently, a judge in the Northern District of Illinois rejected a disclosure-only settlement as a "racket" because the settlement provided the shareholders "nothing of value, and instead caused the company in which they hold an interest to lose money. The quick settlements obviously took place in an effort to avoid the judicial review this decision imposes." *House v Akorn, Inc.*, 385 F. Supp. 3d 616 (N.D. IL 2019). It has been noted that *Trulia* may result in fewer merger-objection lawsuits and has already potentially contributed to a decline in the rate of merger-objection filings. *See*, Boettrich & Starykh, *supra*.

4. Event-Driven Litigation

Event-driven securities lawsuits continue to be one of the trends to watch in the D&O world. These claims result from negative events such as a product failure, plant explosion, data breach, or law enforcement action. The greatest growth can be found in securities lawsuits related to a regulatory action that resulted in a decline in the company's share price. In 2018, Johnson & Johnson disclosed possible asbestos contamination of its baby talcum powder, which caused its stock to drop by 10 percent in one day. A securities class action was filed shortly thereafter.

Other recent examples of event-driven securities litigation relate to the California wildfires. The November 8, 2018 Woolsey and Hill fires resulted in a shareholder suit 8 days later against Southern California Edison Company (SCE), a subsidiary of Edison International alleging that the companies made false and misleading statements or failed to disclose that: (i) the Company failed to maintain electricity transmission and distribution networks in compliance with safety requirements and regulations promulgated under state law; (ii) consequently, the Company was in violation of state law and regulations; (iii) the Company's noncompliant electricity networks created a significantly heightened risk of wildfires in California; and (iv) as a result, the Company's public statements were materially false and misleading at all relevant times. The complaint alleged that following the California Public Utilities Commission's (CPUC) announcement that it was investigating SCE, Edison's share price fell 12% and Edison's share price continued to fall as the fires continued to burn for a total decline of 32% from its price before the CPUC announcement. *Barnes v. Edison Int'l*, No. 2:18-cv-09690 (C.D. CA Nov. 16, 2018).

On October 25, 2019, a securities lawsuit was filed against three executives of PG&E, another California utility company, related to other California wildfires. *Vataj v Johnson*, No. 4:19-cv-06996 (N.D. CA Oct. 25, 2019). This complaint also alleged that the executives had damaged the company by failing to implement precautionary measures to decrease the threat of wildfires in California communities and that PG&E's public statements on its efforts to address wildfire-related threats were false and misleading. One executive was quoted as saying that "[i]n recent years, we've made significant changes and additions to our business to combat these weather events, but the climate is changing faster."

The events that can drive securities litigation are as broad and varied as the creative minds of the plaintiffs' class action bar in conjunction with events both global and domestic. Despite the rise in event-driven securities litigation, courts are confronting these lawsuits with some skepticism. Event-driven securities lawsuits have a dismissal rate approaching 60%, much higher than more traditional securities lawsuits. See, Dailey & Marder, "The Rise of Event-Driven Securities Litigation—Why It Matters to Directors & Officers," www.akingump.com, (2018).

B. Derivative Actions

In the early days of securities litigation, derivative actions were primarily follow-on/ tag-along cases, often swept into the resolution of the "real" case with minimal attention and expense. The dawn of the 21st century also saw a significant rise in these follow-on actions, significant enough to dub the trend a curse. *See*, LaCroix, "A Small Step Toward Curbing the Follow-On Derivative Suit Curse," *The D&O Diary*, (Jan. 30, 2012). A quick review of D&O Diary articles on derivative actions after identifying them as a curse reveals discussions on derivative actions against a long list of major corporations including:

- dismissals of actions against BP and Facebook and the "largest ever" derivative settlement ($139 million) by News Corp. insurers (2013);
- data breach-related derivative actions against Target and Wyndham (dismissed) and the "largest ever" settlement ($275 million) by Activision (2014);
- data breach-related derivative suit against Home Depot (2015);
- dismissals of the Target and Home Depot (appealed) actions and filing of data breach-related case against Wendy's (2016);
- Home Depot settlement and 21st Century Fox sexual misconduct-related derivative settlement ($90 million funded by insurers) (2017);
- Wendy's settlement (remedial measures, data security protocols and $950,000 paid to plaintiffs' attorneys by insurers) and sexual misconduct-related suit against Nike (2018); and
- Sexual misconduct-related action against Alphabet for conduct at Google, Yahoo data breach-related settlement ($29 million), Wells Fargo bogus account scandal settlement ($320 million), and Oracle Special Litigation Committee recommends derivative claims be allowed to proceed (2019).

These derivative action highlights reveal that derivative actions, like their securities partners, are now frequently event-driven. The settlement numbers also reflect that derivative actions have become "real," not just follow-on litigation. There are also more stand-alone derivative actions than in the past, *e.g.* opioids, and nine figure settlements are not uncommon.

These changes in the world of derivative litigation are having a major impact on D&O insurers. Management of derivative claims has become increasingly challenging with the potential exposures dynamically impacting the D&O landscape.

C. Recent SEC Activity

1. Enforcement Actions

New enforcement actions by the Securities and Exchange Commission (SEC) against public companies rose 30% in Fiscal Year 2019. The SEC filed 95 new actions against public companies and subsidiaries in FY 2019, up from 72 in the prior year. It was the highest number in any fiscal year since the Securities Enforcement Empirical Database began tracking the data in FY 2010. See, Cornerstone Research Press Release, www.cornerstone.com, (Nov. 20, 2019). These numbers are significant in that securities litigation may be spurred by SEC actions and findings which frequently relate to corporate failures to make required disclosures. Targeted sectors in 2019 were investment adviser/investment companies, broker dealers, and other defendants in the finance, insurance and real estate industry.

2. Whistleblower Reports and Awards

The number of whistleblower reports and the total value of whistleblower awards also continued at elevated levels in FY 2019. *See*, SEC 2019 Annual Report to Congress, "Whistleblower Program," (Nov. 15, 2019). The 5,212 reports filed represents a slight decline for the first time since the program began. The most common complaints were corporate disclosures and financials, offering fraud, and manipulation. There were 289 crypto currency-related reports and 200 Foreign Corrupt Practices Act related reports. While the Whistleblower Program has led to many successful SEC enforcement actions producing over $2 billion in monetary sanctions, there have been relatively few awards to whistleblowers—only 67 (.2% of all reporters) in the history of the program. *See*, LaCroix, "SEC: Whistleblower Reports and Awards Continue at Elevated Levels," *The D&O Diary*, (Nov. 19, 2019). As with SEC enforcement actions, the whistleblower program provides some potential insight into future securities claims.

II. Cyber/Data/Privacy Exposures

A. D&O Exposures

Cybersecurity presents a significant risk management concern for corporations and has also become a potential source of liability for directors and officers. *See*, Ferillo & Veltsos, "Time to Face the Music—Cyber Risk is D&O Risk—And Things Are Getting Worse!" *The D&O Diary*, (Sept. 3, 2019). The failure of directors and officers to adopt policies and procedures to avoid a cyberattack or data breach will be scrutinized in any shareholder action following a cyber event. The company's response to the incident also has the potential to draw litigation related to disclosures made after the incident.

For example, on June 26, 2019, a securities case was filed against FedEx and its directors and officers alleging that the company had made fraudulent disclosures concerning the extent of the impact of a cyberattack involving the NotPetya malware virus. FedEx assured investors that any negative impact from the attack was minimal, that customers "stuck with us," and that FedEx was "on track" to achieve its integration goals for its multibillion dollar acquisition of TNT. The complaint alleged that as the truth about TNT's deteriorating business and higher than expected integration costs were revealed, FedEx's stock declined and FedEx's shareholders were damaged. *R.I. Laborers' Pension Fund v. FedEx Corp*., No. 1:19-cv-05990 (S.D.N.Y. June 26, 2019).

The SEC issued guidance in February 2018 for cybersecurity disclosures in an attempt to ensure that companies adequately inform shareholders of cybersecurity risks and incidents. The guidance, which has been criticized for its lack of helpful suggestions, does recognize that cybersecurity disclosures are encompassed in the existing U.S. securities laws and requirements and explains that "although no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, companies nonetheless may be obligated to disclose such risks and incidents." "Given the frequency, magnitude and cost of cybersecurity incidents,…it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack." Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459, 34-82746 (Feb. 21, 2018), www.sec.gov.

Subsequent to issuing its guidance, the SEC levied a $35 million penalty against Yahoo's successor for a two-year delay in disclosing its 2014 massive data breach. *See*, Hamm, "Cybersecurity: Where Are We, and What More Can Be Done*?*," CPA J. (Sept. 2019). While the breach was reported to Yahoo's senior management and legal department, the company allegedly failed to properly investigate the incident or consider whether it should be disclosed to investors. Yahoo had previously paid $29 million to settle a shareholder derivative action alleging that former directors and officers had failed to properly oversee the company's handling of a series of cyberattacks occurring between 2013 and 2016 and in 2018, Yahoo also paid $80 million to settle a securities lawsuit relating to the cyberattacks.

Equifax also found itself in securities litigation following its September 2017 announcement of a "cybersecurity incident" potentially impacting 143 million U.S. customers The plaintiffs alleged that Equifax had issued materially false or misleading statements or did not disclose that it failed to maintain adequate measures to protect its data system, failed to maintain adequate monitoring systems to detect security breaches, and failed to maintain proper security systems, controls and monitoring systems in place. The complaint also alleged that, just days after the company discovered the data breach, Equifax executives sold off company stock and that Equifax stock value declined nearly 17% following disclosure of the data breach. *Kuhns v. Equifax Inc.,* No. 1:17-mi-99999 (N.D. Ga. Sept. 8, 2017).

Other significant cyber event-related claims worthy of note for corporate officers and boards of directors are the Capital One massive data breach, the Marriott International data breach, the Zendesk data breach, and Facebook's privacy-related securities class action.

B. Cyber Policy Exposures

Cyber policies are no longer a new line of products but they are still not widely understood. As described below, cyber coverage is often mistakenly sought for losses insured by more traditional policies such as crime coverage simply because the occurrence or claim involves some technological aspect. The nature and scope of available coverages under cyber policies are beyond the scope of this presentation but, given the huge exposures to corporations and corporate management from the broad scope of cyber-related threats and risks, exploration and evaluation of available cyber coverages is now a key aspect in reviewing an insurance program for corporations.

C. Other Policy Exposures

The well-publicized 2014 Target data breach resulted in massive losses to the company. Apparently Target had a $90 million cyber insurance program which was exhausted by payment of losses resulting from the data breach. *See*, LaCroix, "Seeking Insurance for Cybersecurity-Related Losses," *The D&O Diary*, (Nov. 24, 2019). This post from LaCroix's D&O blog chronicles the efforts of insureds to find coverage for cyber-related losses. In addition to Target's effort to find coverage for its data breach losses under its general liability (GL) policy, the blog discusses the Mondelez action against Zurich to recover under a property policy for losses from the NotPetya virus attack on IT systems. An attempt to find coverage under a professional liability policy for a payment instruction fraud claim is also referenced.

Payment instruction fraud is a trending issue which raises coverage questions as it is a cyber event which intuitively seems like it would be a cyber claim. *See*, Floresca, "Payment Impersonation Fraud: Why is This Common Cyber Problem Not a Valid Cyber Claim?" www.woodruffsawyer.com, (Dec. 5, 2019). Floresca states that the underwriting for these claims is really about accounting controls, *i.e.* crime, rather than IT security, *i.e.* cyber, and coverage for these losses should be found in the insured's crime policy. Or, from the broker's view, find a way to add coverage under both policies. *See also*, LaCroix, "Payment Instruction Fraud and Cyber Insurance Coverage," *The D&O Diary*, (Dec. 9, 2019).

"Silent cyber" is an insurance industry commentator moniker to describe the possibility that insurance coverage for cyber-related losses may be found in various policies in an insured's program. Given the new frontier of potential cyber events, claims, and resulting exposures, the search for coverage for cyber-related losses has just begun.