October 15, 2024

Q3 2024 U.S. Legal & Regulatory Developments

The following is our summary of significant U.S. legal and regulatory developments during the third quarter of 2024 of interest to Canadian companies and their advisors.

1. SDNY Court Deals Blow to SEC Cyber Enforcement, Dismisses Most Charges Against SolarWinds and Its CISO

On July 18, 2024, Judge Paul A. Engelmayer of the U.S. District Court for the Southern District of New York ("SDNY") granted in large part a motion by SolarWinds Corporation ("SolarWinds") and Timothy Brown, SolarWinds' Chief Information Security Office ("CISO"), to dismiss a civil suit filed against them by the Securities and Exchange Commission ("SEC"). The motion to dismiss was supported by four groups that submitted amicus briefs, including a brief submitted by Paul, Weiss on behalf of former government officials.

According to the SEC's lawsuit, in January 2019, threat actors secured access to SolarWinds' corporate VPN and proceeded to exploit that connection to access SolarWinds' network. The threat actors subsequently inserted malicious code into SolarWinds' software. The threat actors leveraged this malicious code to conduct a series of cyberattacks, later referred to as SUNBURST, which impacted the operations of many of SolarWinds' customers, including federal and state government agencies. After learning of the SUNBURST attack, Brown and other executives at SolarWinds prepared Form 8-K filings disclosing the event. On October 30, 2023, the SEC brought securities fraud claims against SolarWinds and Brown based on alleged material omissions and misstatements in disclosures that were made in public statements and in SEC filings both before and after the SUNBURST attack.

When filed, the case marked a number of firsts for the SEC: the first time it had brought intentional fraud charges in a cybersecurity disclosure case, the first time it had brought an accounting control claim based on an issuer's alleged cybersecurity failings, and the first time it had brought a cybersecurity enforcement claim against an individual. The SEC based its claims on alleged material misrepresentations and omissions by SolarWinds and Brown, both before and after the company disclosed a large-scale cyberattack, known as SUNBURST, in December 2020. Specifically, the SEC alleged that SolarWinds and Brown had misleadingly touted the company's cybersecurity practices before the incident, including in a security statement published on the company's website, in a cybersecurity risk disclosure made in SolarWinds' SEC filings, and in press releases, podcasts and blog posts. The SEC also alleged that the company's Form 8-K disclosures following the SUNBURST incident minimized the scope and severity of the attack. Additional claims were premised on SolarWinds' purported failure to maintain effective internal accounting and disclosure controls and procedures for identifying and disclosing cybersecurity risks.

The only set of claims sustained by the court were the claims against SolarWinds and Brown for securities fraud based on the security statement on the company's website, which claims the court held were viably pled as materially false and misleading in numerous respects. The court dismissed the claims of securities fraud and of false filings based on other statements and filings,

as well as all of the claims based on SolarWinds' post-SUNBURST disclosures. The court also dismissed the SEC's claims relating to SolarWinds' internal accounting and disclosure controls and procedures.

Key Takeaways

- Specific false or misleading statements on a company's public website about the state of a company's cybersecurity, even if the statements are directed to customers rather than investors, can be the basis for securities fraud liability: The court declined to dismiss the SEC's claims related to a security statement published on a SolarWinds website, explaining that the statement was accessible to investors and therefore part of the "total mix of information" that SolarWinds furnished to the investing public. According to the amended complaint, Brown approved and disseminated the security statement despite being privy to internal information that contradicted the statement's representations about the company's access controls and password practices. The court determined that the alleged misrepresentations, as pled, were materially misleading and that the allegations sufficiently pleaded Brown's knowledge of, or at least recklessness as to, the misstatements on SolarWinds' website. Additionally, the court concluded that Brown's scienter was properly imputed to SolarWinds. Although it remains to be seen whether the evidence will support the allegations, the fact that these claims based on a public security statement were the only claims to survive the motion to dismiss, serves as an important reminder that all public statements about a company's cybersecurity practices, not only those in SEC filings, can have legal consequences and should therefore be carefully reviewed for accuracy.

- "Internal accounting controls" do not extend to cybersecurity controls: The court held that Section 13(b)(2)(B) of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), which requires an issuer to devise and maintain "internal accounting controls," is limited to controls related to accounting and does not extend to cybersecurity controls, such as password and VPN protocols. As the court explained, the Exchange Act "does not govern every internal system a public company uses to guard against unauthorized access to its assets, but only those qualifying as 'internal accounting' controls." "Cybersecurity controls," stated the court, "are undeniably vitally important, and their failures can have systemically damaging consequences. But these controls cannot fairly be said to be in place to 'prevent and detect errors and irregularities that arise in the accounting systems of the company.'"

If the decision stands, it could limit the SEC's ability to pursue Exchange Act claims related to internal controls that do not relate specifically to the company's financial statements. And the SEC could therefore lose an important tool for public company cybersecurity enforcement. Just last month, the SEC announced that R.R. Donnelley & Sons Co. had agreed to pay $2.1 million to settle charges that the company failed to maintain "cybersecurity-related internal accounting controls" and to design effective disclosure controls to report relevant cybersecurity information to management. The SolarWinds decision may make it more difficult for the SEC to settle internal accounting controls claims based on allegedly deficient cybersecurity controls.

- **Cybersecurity risk disclosures and disclosure controls can provide important defenses to securities fraud claims**: The court reiterated that risk disclosures do not need to be stated with maximum specificity and detail under the securities laws, and found that SolarWinds had adequately identified in its disclosures the nature and types of cyber risks that it faced and associated consequences. Moreover, the court seemed to attach significance to SolarWinds' ability to promptly assess whether disclosures of material information to the investing public were needed, and to file a Form 8-K disclosing the cyberattack within a matter of days. In the court's view, "[p]erspective and context are critical" when evaluating whether SolarWinds' Form 8-K was sufficiently pled as materially misleading; considering the "short turn-around" in which SolarWinds was able to file its Form 8-K disclosing the SUNBURST attack, it contained "appropriate gravity and detail."

For the full text of our memorandum, please see:

- https://www.paulweiss.com/practices/litigation/cybersecurity-data-protection/publications/sdny-court-deals-blow-to-sec-cyber-enforcement-dismisses-most-charges-against-solarwinds-and-its-ciso?id=52318

For the district court's opinion in *SEC* v. *SolarWinds Corp. & Timothy Brown*, please see:

- https://www.nysd.uscourts.gov/sites/default/files/2024-07/SolarWinds%20Opinion%20%28Dkt.%20125%29.pdf

2. DOJ Launches New Whistleblower Program Focused on Corporate Misconduct

On August 1, 2024, the U.S. Department of Justice's Criminal Division ("DOJ" or "Department") launched a new Corporate Whistleblower Awards Pilot Program (the "Whistleblower Pilot Program" or the "Pilot Program"). The launch of the Whistleblower Pilot Program follows DOJ's announcement of the program in March. The Pilot Program will be managed by the Criminal Division's Money Laundering and Asset Recovery Section. DOJ plans to "regularly assess the design and implementation of the Pilot Program and, at the end of this 3-year pilot period, the Department will determine whether the program will be extended in duration or modified in any respect."

Under the Pilot Program, eligible whistleblowers who provide DOJ's Criminal Division with original and truthful information about certain types of corporate misconduct are eligible to receive a portion of a criminal or civil forfeiture exceeding $1 million. The Pilot Program covers certain crimes involving financial institutions, domestic or foreign corruption by companies and health care fraud schemes involving private insurance plans.

DOJ has in recent years offered increased incentives to companies that self-report corporate misconduct. Under a 2022 revision to DOJ's voluntary disclosure policy, absent aggravating factors, "the Department will not seek a guilty plea when a company has voluntarily self-disclosed, cooperated, and remediated misconduct." This policy provides considerable benefits to eligible companies that file a Voluntary Self-Disclosure ("VSD"), including a potential declination.

However, DOJ has made clear that it is also seeking to incentivize individuals to come forward with original information about corporate misconduct. Under the Individual VSD Program announced in April 2024, certain individuals who were involved in corporate misconduct are eligible to receive a Non-Prosecution Agreement ("NPA") if they report information to DOJ and cooperate in the investigation. Now, under the Whistleblower Pilot Program, eligible individuals are financially incentivized to report corporate misconduct to DOJ's Criminal Division. While the Individual VSD program applied only to individuals involved in the misconduct, the Whistleblower Pilot Program more broadly offers an incentive to eligible individuals to report corporate misconduct to DOJ.

The Deputy Attorney General noted that there is "a synergy to these disclosure programs: together, they create a multiplier effect that encourages both companies and individuals to tell us what they know — and to tell us as soon as they know it." In order for the individual to receive an NPA or whistleblower reward, they must generally report original information that DOJ did not have before. As the Deputy Attorney General noted, "to be eligible for the most significant benefits under these disclosure programs — both our corporate voluntary self-disclosure programs and the whistleblower initiative we're announcing today — you have to tell us something we didn't already know. With very few exceptions, you need to be first in the door."

Amendment to Corporate VSD Policy

Alongside the Whistleblower Pilot Program, DOJ announced that it was amending its VSD policy for corporations. "Under that amendment, where a company receives an internal report from a whistleblower, if the company comes forward and reports the misconduct to the Department within 120 days and before the Department reaches out to the company, the company will be eligible for the greatest benefit under our policy—a presumption of a declination—so long as they fully cooperate and remediate." This amendment is designed to incentivize companies to file VSDs where they receive a report from a whistleblower—and they can still receive the "greatest benefits" under the policy if they file the VSD within 120 days and before DOJ has reached out to the company about the issue. This is designed to create an incentive for companies to come forward with whistleblower allegations, rather than deal with them exclusively internally.

Confidentiality and Retaliation
Similar to other whistleblower programs, the Pilot Program affords whistleblowers confidentiality protections. Under the program, DOJ will "not publicly disclose any information, including information . . . that could reasonably be expected to reveal the identity of a whistleblower, except as required by law or Department policy as determined by the Department, in its sole discretion, unless and until required to be disclosed to a defendant in connection with a judicial or administrative proceeding."

While the program does not afford explicit anti-retaliation protections to whistleblowers, DOJ notes that any retaliation would be assessed in terms of whether the company or any individual "cooperated with the Department or obstructed an investigation" and DOJ could "institute appropriate enforcement actions in response to retaliation."

Compliance Considerations
With the adoption of the Whistleblower Pilot Program and the corresponding update to the corporate VSD Policy, it is clear that DOJ is continuing to aggressively incentivize individuals and companies to provide the Department with information about certain corporate misconduct. As a result, there are a number of steps that companies may wish to consider to respond to the increased risk of a whistleblower report to DOJ:

- *First*, companies may wish to review their internal investigation protocols and related statistics, including the average run time for their investigations. They may wish to consider policy or process changes to ensure that going forward, potentially reportable matters are timely triaged and investigated. For example, companies may wish to consider making adjustments to their intake process, such as their risk ranking or prioritization criteria, and/or establish target guidelines for completing certain investigatory phases within the 120-day window.

- *Second*, companies may wish to review their whistleblower and anti-retaliation policies and ensure that their reporting channels are both easily accessible and sufficiently advertised. Companies may also wish to consider developing or revising their guidelines for responding to and communicating with whistleblowers—in accordance with anti-retaliation protections—to address the risk that colleagues may be operating as external whistleblowers.

- *Third*, companies may wish to consider developing a framework for determining when it will report matters to DOJ and who will be involved in those decisions, and at what stage they will consult external counsel.

For the full text of our memorandum, please see:

- https://www.paulweiss.com/practices/litigation/economic-sanctions-aml/publications/doj-launches-new-whistleblower-program-focused-on-corporate-misconduct?id=53518

For DOJ's program guidance on the Whistleblower Pilot Program, please see:

- https://www.justice.gov/criminal/media/1362321/dl?inline

3. CFIUS Releases 2023 Annual Report, Highlighting Enforcement Activity

On July 23, 2024, the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") released its most recent annual report (the "Report"), covering the Committee's activities for calendar year 2023. The Report provides the public with information about the number of transactions reviewed by the Committee, outcomes of reviews and the industries and foreign countries associated with its reviews.

Although comprising largely statistical information and not providing details on the specific considerations involved in a given review, the Report offers a number of insights which we explore below.

Despite Lower Case Numbers, CFIUS Remains a Robust Regulatory Program
In 2023, parties filed 233 "notices" and 109 "declarations" with the Committee, compared to 286 notices and 154 declarations in 2022. Although the total number of filings—both short-form "declarations" and long form "notices"—was down year-over-year from 2022, the number of filings the Committee reviews each year has more to do with overall global merger and acquisition activity and less to do with whether the Committee has tempered its recent trend of being an active and engaging national security regulator.

The slight statistical downtick in the Report should not therefore be viewed in a vacuum. For example, CFIUS activity for the last three years as reported in its annual reports (i.e., calendar years 2021–2023), shows the Committee consistently reviewing hundreds of unique transactions a year. Further, as discussed below, when the Committee's "non-notified" review activities are factored in, it can be said that CFIUS is now screening thousands of transactions per year in one form or another.

CFIUS therefore remains an important regulatory consideration for dealmakers.

The Declaration Program Has Matured into a Real Option, at Least for Lower Risk Investors
A creation of the Foreign Investment Risk Review Modernization Act of 2018, the declaration program provides transacting parties with a "short-form" filing option that is evaluated on an expedited, 30-day timeline. Filers that chose the declaration option have the chance to obtain a clearance much faster than they would by filing a notice, but declarations also carry the risk of a longer process because CFIUS may conclude its review of a declaration by requesting that the parties file a long-form notice. In other words, if the conclusion of the declaration process is unfavorable, parties may find themselves back to square one in their CFIUS regulatory process.

CFIUS requesting that declaration filers thereafter submit notices is not an infrequent occurrence. In calendar year 2022, declaration filings resulted in notice requests 32% of the time (a significant increase from 2021's 19% rate). In 2023, the rate of notice requests dropped down to 21% (i.e., 20 such requests out of 109 declarations). Averaging calendar years 2021–2023 together, the notice request rate stands at approximately 25%. In other words, over the last three years covered by CFIUS's annual reports, about 75% of declarations were able to achieve a successful outcome.

Although a decision whether to file a declaration or a notice should only be made after assessing the specifics of the transaction with CFIUS counsel, it is clear that the declaration program has become a viable approach to obtaining CFIUS clearance—and obtaining it quickly—in many cases. This is particularly true for investors originating from countries that are strategic allies of the United States. It is therefore no surprise that Canada, the United Kingdom and Japan were the largest source of declaration filers, with Australia, France and South Korea close behind.

Timing and Efficiency Has Improved, but Is Still a Challenge in Many Transactions
In 2022, 57% of notices extended into the second 45-day "investigation" period (up from 48% in 2021), and 31% of notices were withdrawn (versus 26% in 2021). At least some of the withdrawn notices were subsequently refiled, meaning that, for a number of transactions, the CFIUS process extended well beyond the 90 days typically allotted for a filing.

In 2023, CFIUS reviewed 233 notice filings. Of those, 128, or 54%, progressed into the second 45-day investigation period. This represents a slight, 3%, reduction compared to the number of reviews that progressed into the second stage in 2022, but is more than the 47% rate in 2021. Indeed, 2022–2023 represent a reversal of what had been a lengthy trend dating back to 2015 wherein a majority of notices were cleared in the first review period. Further, the Report states that, in 2023, 57 notices were withdrawn after commencement of investigation. This equates to approximately 25% of all notices, which again represents only a relatively modest improvement over the 31% of withdrawn notices in 2022.

Undoubtedly, CFIUS's efficiency improved in 2023 compared to the year before. But, a significant number of notice filings continue to result in lengthy review processes. Fewer than half of all notices clear in the first 45-day review period. A substantial percentage of notices, nearly a quarter, must be withdrawn after going through the 90-day process (i.e., the 45-day review

followed by a 45-day investigation). Although some of those transactions are abandoned, as discussed below many of them will ultimately be cleared by CFIUS. This means that, in complex transactions, parties should anticipate processes that may extend well beyond 90 days.

Mitigation (and Abandonments) Remain Common
In addition to timing considerations, parties must continue to consider the likelihood that CFIUS will only clear their transaction if it is conditioned on a mitigation agreement, as well as the potential that CFIUS will decide that security risks cannot be mitigated, thus forcing the parties to abandon their transaction outright.

In 2023, CFIUS required mitigation as a condition of its approval in 35 cases, or approximately 21% of all distinct transactions. This is a substantial number consistent with recent trends. Further, the Report notes that in nine cases, parties abandoned their transactions after being informed by CFIUS that the Committee could not identify any acceptable measures to mitigate threats to U.S. national security. In another five cases, parties abandoned transactions for commercial reasons (of which timing could have been a consideration).

A substantial number of transactions could only obtain clearance after the parties agreed to mitigate national security risks that the Committee had identified, and a number of other transactions had to be abandoned by their parties outright. Particularly with CFIUS's emphasis on enforcement and its increased use of civil monetary penalties, parties must carefully consider the range of potential mitigation outcomes before entering into a transaction. Even in lengthier reviews, parties often have only days or weeks to negotiate the terms of mitigation agreements (and CFIUS has proposed changes to its regulations which could further limit the parties' time to negotiate agreements), so thoughtful preparation for mitigation scenarios is critical to successfully navigating the CFIUS process.

CFIUS Is Following Through on Tougher Enforcement Talk
In 2023, the Committee assessed four civil monetary penalties for breaches of material provisions in mitigation agreements—double the total number of such penalties issued by CFIUS in its entire 50-year history up to that point. On top of these penalties, the Report touts other aspects of the Committee's focus on enforcement. CFIUS conducted 43 site visits to assess the parties' compliance with their mitigation agreements and now routinely requires the parties to mitigation agreements to establish formal compliance plans. As part of its oversight activities, the Committee undertook "several" investigations related to compliance, some of which identified instances of noncompliance which were addressed through measures other than civil monetary penalties.

The Report also indicates that CFIUS continues to aggressively search for non-notified transactions, particularly those that may have been subject to mandatory filing. CFIUS now screens "thousands" of transactions as part of its effort to identify potential non-notified transactions worthy of investigation and, in 2023, opened formal non-notified inquiries for 60 transactions, requesting notice filings for 13 of those.

Looking forward, it seems that CFIUS will continue to focus on enforcement efforts. The U.S. Department of the Treasury ("Treasury") recently proposed new rules that would increase CFIUS's information collection authority regarding non-notified transactions, as well as its authority to levy penalties. Treasury also proposed a new rule that would vastly expand CFIUS jurisdiction over certain real estate transactions near military installations.

For the full text of our memorandum, please see:

- https://www.paulweiss.com/practices/litigation/national-security-cfius-fara/publications/cfius-releases-2023-annual-report-highlighting-enforcement-activity?id=53606#_ftn7

For the full text of our 2023 CFIUS, Outbound Investments, and Export Control Year in Review, please see:

- https://www.paulweiss.com/media/3984128/2023_year_in_review_cfius_outbound_investments_and_export_controls.pdf

For the 2023 CFIUS Annual Report, please see:

- https://home.treasury.gov/system/files/206/2023CFIUSAnnualReport.pdf

4. FTC Non-Compete Clause Rule Is Set Aside by Court

On August 20, 2024, in *Ryan LLC, et al.* v. *Federal Trade Commission* No. 24-cv-986 (N.D. Tex. Aug. 8, 2024) ("*Ryan*"), a federal district court in Texas ruled on the merits that the Federal Trade Commission ("FTC") does not have statutory authority to promulgate its non-compete clause rule (the "Non-Compete Clause Rule") and that the rule is arbitrary and capricious. As a consequence, the court set aside the rule under the Administrative Procedure Act and ordered that it "shall not be enforced or otherwise take effect." The order is nationwide in scope and not party-specific. One other challenge to the rule is pending in another district court. To the extent those actions produce inconsistent orders, it will be up to the courts of appeals and ultimately the United States Supreme Court to either maintain the district court's order or allow the rule to go into effect.

Possible Scenarios Going Forward

Further Legal Proceedings Regarding the Rule

In a statement released shortly after the Texas court's ruling, an FTC spokesperson said that the Commission is "seriously considering a potential appeal." An appeal of the *Ryan* decision could introduce a number of uncertainties as to timing and the effect of interim relief, if any, pending appeal. In addition, two other actions challenging the rule are pending in district courts in two different circuits. This could potentially lead to a circuit split. In *ATS Tree Services, LLC* v. *Federal Trade Commission, et al.*, No. 24-cv-1743 (E.D. Pa. July 23, 2024) ("*ATS Tree Services*"), the court denied the plaintiff's motion for stay of effective date and preliminary injunction. The parties to that action have requested that the court enter a summary judgment briefing schedule that would continue through October. More recently, on August 15, 2024, the court in *Properties of the Villages* v. *Federal Trade Commission*, No. 24-cv-316 (M.D. Fla. June 21, 2024), granted the plaintiff's motion for stay and preliminary injunction, but limited this relief to the named plaintiff. That court has yet to order a schedule for further proceedings.

Enforcement Against Non-Competes Through Individual Adjudication

The FTC spokesperson said that the agency "will keep fighting to stop non-competes that restrict the economic liberty of hardworking Americans, hamper economic growth, limit innovation, and depress wages" and that the "decision does not prevent the FTC from addressing non-competes through case-by-case enforcement actions." The FTC has asserted that non-competes are unfair methods of competition under section 5 of the Federal Trade Commission Act of 1914 (the "FTC Act") and that it is consequently empowered to "prevent" entities under its jurisdiction from "using" them. The FTC asserted this power in several adjudicative actions just prior to the promulgation of the Non-Compete Clause Rule, but these were resolved on consent and the FTC's asserted authority in this area has not been tested by an adversarial proceeding on the merits. Notably, the court in the *ATS Tree Services* action in Pennsylvania, found "that the FTC acted within its authority under the [FTC] Act in designating all non-compete clauses as unfair methods of competition." Also, under certain circumstances a non-compete agreement may be found to violate the rule of reason under section 1 of the Sherman Antitrust Act of 1890. There are also numerous state laws regulating non-competes.

For the full text of our memorandum, please see:

- https://www.paulweiss.com/practices/litigation/antitrust/publications/ftc-non-compete-clause-rule-is-set-aside-by-court?id=53676

For the full text of our memorandum on the FTC's final rule, please see:

- https://www.paulweiss.com/practices/litigation/antitrust/publications/ftc-issues-final-rule-banning-employer-worker-non-competes-and-is-immediately-challenged-in-court?id=51184

For the district court's opinion in *Ryan LLC, et al.* v. *FTC*, please see:

- https://law.justia.com/cases/federal/district-courts/texas/txndce/3:2024cv00986/389064/211/

5. Delaware Supreme Court Clarifies Tests for Advance Notice Bylaw Challenges

In *Kellner* v. *AIM ImmunoTech, Inc.* ("*Kellner*"), the Delaware Supreme Court clarified the legal tests applicable when stockholders challenge advance notice bylaws. A key aspect of the Supreme Court's ruling is the importance of distinguishing between a facial and an as-applied challenge to a bylaw. The court held that advance notice bylaws, like all corporate bylaws, are presumptively valid under Delaware law and will survive a facial challenge if they (1) are consistent with the company's charter, (2) are not prohibited by law and (3) address a proper subject matter. Stated differently, a bylaw is facially invalid only if it cannot operate lawfully under any circumstance. An as-applied challenge, by contrast, considers whether the board adopted or enforced a bylaw inequitably in a specific circumstance. As-applied challenges are reviewed under enhanced scrutiny and can—if the balance of the equities so require—result in the board being enjoined from enforcing the bylaw against the specific plaintiff-stockholder bringing the challenge.

Nevertheless, because of the proxy contestants' own deceptive conduct, the court ruled that no remedy was warranted in equity.

Takeaways

The Supreme Court's *Kellner* decision confirms that, while directors have flexibility in designing bylaws, including advance notice requirements, those bylaws remain susceptible to judicial review for strict legal compliance. And the directors remain susceptible to claims for breach of the fiduciary duty of loyalty if they employ those bylaws inequitably. To satisfy these requirements, drafters of bylaws and directors adopting them should, among other things, consider the clarity of advance notice bylaws as drafted. Directors should also consider whether an advance notice bylaw embodies a proper and equitable purpose, such as ensuring an orderly and fair election where information is disclosed in a timely manner so as to permit stockholders to consider the competing arguments on both sides.

For the full text of our memorandum, please see:

- https://www.paulweiss.com/media/3985034/delaware_supreme_court_clarifies_tests_for_advance_notice_bylaw_challenges.pdf

For the Delaware Supreme Court's opinion in *Kellner* v. *AIM ImmunoTech, Inc.*, please see:

- https://courts.delaware.gov/Opinions/Download.aspx?id=366380

6. Delaware Court of Chancery Holds Charters Cannot Incorporate Private Agreements by Reference

In *Seavitt* v. *N-able, Inc.* ("*Seavitt*"), the Delaware Court of Chancery (in an opinion by Vice Chancellor Laster) held that the charter of a Delaware corporation cannot incorporate by reference the substantive terms of a stockholders or other private agreement. According to the court, allowing parties to do so "introduces the DNA of a purely private agreement into a foundational and public document." Further, because parties could amend such agreements without a stockholder vote, and thereby automatically change the charter's substantive terms, allowing private agreements' incorporation into a charter would deprive stockholders of their statutory right to vote on charter amendments under the Delaware General Corporation Law (the "DGCL").

The above holding arose in the context of an opinion that invalidated governance rights in a stockholders agreement in accordance with *W. Palm Beach Firefighters' Pension Fund* v. *Moelis & Co.* ("*Moelis*") and *Wagner* v. *BRP Grp., Inc.* ("*BRP*"). As acknowledged by the court, the analysis resulting in the invalidation of the stockholders agreement provisions would not apply once the 2024 amendments to the DGCL went into effect on August 1, 2024. However, the 2024 DGCL amendments would not affect the court's holding that incorporation by reference of the terms of a private agreement into a charter is invalid. Parties drafting charter provisions should consider this case carefully to ensure that desired substantive terms receive their intended effects, such as by minimizing references to external private agreements and including substantive provisions in the charter itself to the extent feasible in the circumstances.

For the full text of our memorandum, please see:

- https://www.paulweiss.com/practices/transactional/mergers-acquisitions/publications/delaware-court-of-chancery-holds-charters-cannot-incorporate-private-agreements-by-reference?id=53442

For the Delaware Court of Chancery's opinion in *Seavitt* v. *N-able, Inc.*, please see:

- https://courts.delaware.gov/Opinions/Download.aspx?id=367070

For the full text of our memorandum on the 2024 Amendments to the DGCL, please see:

- https://www.paulweiss.com/media/3984934/delaware_general_assembly_approves_2024_amendments_to_general_corporation_law.pdf

7. Delaware Court of Chancery Finds Pharma Buyer Failed to Use Commercially Reasonable Efforts in Achieving Post-Closing Milestones

In a post-trial opinion, the Court of Chancery provides helpful guidance to parties negotiating and drafting contingent value right ("CVR") provisions in acquisition agreements. In *Shareholder Representatives LLC* v. *Alexion Pharmaceuticals, Inc.* ("*Alexion*"), the court found that a pharmaceutical buyer was liable to the stockholder representative of a drug developer seller for (i) a $130 million earnout payment for achieving the first of eight milestones and (ii) failing to use commercially reasonable efforts, as that term was defined in the merger agreement, when it terminated the drug development, with damages to be determined in a forthcoming opinion.

Takeaways

Alexion provides important practical guidance to both acquirors and sellers in the diligence, negotiation and drafting of CVR provisions in acquisition agreements:

- *First,* CVR milestones of scientific, clinical or technical matters should be carefully drafted with inputs from subject matter experts to minimize the risk of disputes and costly litigation. As one illustrative lesson from *Alexion*, despite the highly technical definition and the parties' respective position that the first criterion, which required achieving "an observed PK/PD profile that supports weekly or less frequent subcutaneous administration in long term safety and efficacy studies," was unambiguous, the court nevertheless found the definition ambiguous and reviewed extensively the extrinsic evidence to determine the contracting parties' intentions.

- *Second,* whether to use an outward-facing/objective or an inward-facing/subjective standard for commercially reasonable efforts remains a critical decision in negotiating acquisition agreements. An acquiror should be thoughtful before agreeing to an outward-facing standard, given the unique character of drug development and its company-specific considerations that may not be shared by its similarly situated peers. If and when an acquiror decides to accept an outward-facing standard, however, it should be cognizant of both (i) the practices of its peer group for similar product development, and (ii) the narrow circumstances of subjective factors appropriate for integration into the overall objective standard.

- *Third,* a subjective CVR standard remains valuable in reducing the risk that hypothetical standards and practices of evaluating products will be applied to assessing an acquiror's conduct and compliance with its covenant to use commercially reasonable efforts.

- *Fourth,* regardless of using an objective or subjective standard for CVR, it is important to ensure that such standard reflects the specific, unambiguous criteria the company would use to evaluate continuing or terminating a product development.

- *Fifth,* diligence and understanding of a target company's existing CVR obligations to third parties should remain a front and center consideration for acquirors, particularly acquirors of pharmaceutical companies.

For the full text of our memorandum, please see:

- https://www.paulweiss.com/practices/transactional/mergers-acquisitions/publications/delaware-court-of-chancery-finds-pharma-buyer-failed-to-use-commercially-reasonable-efforts-in-achieving-post-closing-milestones?id=54560

For the Delaware Court of Chancery's opinion in *Shareholder Representatives LLC* v. *Alexion Pharmaceuticals, Inc.*, please see:

- https://courts.delaware.gov/Opinions/Download.aspx?id=369130

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Matthew W. Abbott
+1-212-373-3402
mabbott@paulweiss.com

Andre G. Bouchard
+1-302-655-4413
abouchard@paulweiss.com

Christopher J. Cummings
+1-212-373-3434
ccummings@paulweiss.com

Adam M. Givertz
+1-212-373-3224
agivertz@paulweiss.com

Ian M. Hazlett
+1-212-373-2562
ihazlett@paulweiss.com

Christian G. Kurtz
+1-416-504-0524
ckurtz@paulweiss.com

Audra J. Soloway
+1-212-373-3289
asoloway@paulweiss.com

Stephen C. Centa
+1-416-504-0527
scenta@paulweiss.com

Rosita Lee
+1-212-373-3564
rlee@paulweiss.com

Andrea Quek
+1-416-504-0535
aquek@paulweiss.com

Associates Robin Chang and Thea Winterton-Perks and law clerk Jeremy Jingwei contributed to this Client Memorandum.