PAUL HASTINGS

July 2024

Public Company Watch

Key Issues Impacting Public Companies

SEC Spotlight

SEC Staff Statement on Regulation FD Issues Around Cybersecurity Disclosure

On June 20, 2024, Erik Gerding, Director of the SEC's Division of Corporation Finance, issued a **statement** addressing concerns from companies that the disclosure of certain information about a material cybersecurity incident to commercial counterparties beyond what is disclosed in Item 1.05 of Form 8-K may implicate Regulation FD. Regulation FD requires public disclosure of any material nonpublic information that has been selectively disclosed to certain covered persons, including securities market professionals or shareholders, subject to certain exclusions.[1]

The SEC Staff acknowledged that there are circumstances where sharing additional information on a material cybersecurity incident beyond what was disclosed in Item 1.05 with commercial counterparties or other third-parties may be necessary to convey an impact or risk stemming from the incident to another party, get assistance with mitigation, remediation or avoidance of a future risk, or to allow for a third-party's compliance with their own reporting obligations under SEC rules. The SEC Staff statement reiterated that nothing in the cybersecurity rules alters how communications are treated under Regulation FD and, as with the sharing of any nonpublic information, whether such information sharing falls within the scope of Regulation FD depends on whether such information is material, to whom it is disclosed and whether an exclusion from the rules of Regulation FD applies.

When a company shares private information with third-parties beyond what was disclosed in Item 1.05, they should first look to whether such information is material, since Regulation FD only applies to *material* nonpublic information. Just because the cybersecurity incident at issue was material and, as such, was required to be disclosed in Item 1.05, does not necessarily mean that any additional information that was not publicly disclosed is, in and of itself, material. If the additional nonpublic information is material, the company should then look to whether the third-parties with whom it is sharing the information are the type of persons covered by Regulation FD (i.e., securities market professionals or shareholders). Even if these two conditions are met, there are still exceptions from the application of Regulation FD, for example, if the information is shared with persons who owe a duty of trust or confidence to the company or if such persons agree to keep the information in confidence through a confidentiality agreement.

1 65 Fed. Reg. 51716 (August 24, 2000).

In This Edition

As such, the SEC Staff statement serves to remind companies that Regulation FD should not impede companies from sharing private information related to a material cybersecurity incident if such information sharing is necessary or beneficial and does not fall within the scope of Regulation FD. The cybersecurity rules and Item 1.05 do not alter the usual, well-worn analysis around the requirements of Regulation FD when it comes to the disclosure of material nonpublic information.

SEC Staff Issues New Compliance and Disclosure Interpretations Related to Cybersecurity Rules

On June 24, 2024, the Staff of the SEC's Division of Corporation Finance issued five new compliance and disclosure interpretations ("C&DIs") addressing disclosure under Form 8-K Item 1.05 of material cybersecurity incidents related to ransomware attacks.

The C&DIs address the following issues:

- **Question 104B.05**: Whether a registrant that experiences a ransomware attack is still required to make a materiality determination regarding the incident after a ransomware payment is made and the incident is resolved.

  The Staff notes that the resolution or cessation of a cybersecurity incident that the registrant has not yet determined is material does not relieve the registrant from determining the materiality of the incident after the fact. Item 1.05 requires registrants to determine whether a cybersecurity incident is material, regardless of whether it has been resolved. Moreover, the Staff notes that the fact that the incident has ceased or has been resolved does not necessarily mean that the incident is not material.

- **Question 104B.06**: Whether a registrant must disclose in Item 1.05 a *material* cybersecurity incident involving ransomware when the incident is resolved and ceases before the deadline for reporting material cybersecurity incidents pursuant to Form 8-K.

  The Staff notes that the registrant is required to report such an incident in Item 1.05 because it experienced a cybersecurity incident that it determined to be material. Regardless of whether the incident is ongoing, the registrant must disclose the incident pursuant to Form 8-K within four business days of determining that it was a material cybersecurity incident.

- **Question 104B.07**: Whether the full or substantial reimbursement of a ransomware attack payment pursuant to a registrant's insurance policy covering cybersecurity incidents renders the incident necessarily immaterial.

  The Staff notes that the reimbursement of a ransomware payment pursuant to an insurance policy does not necessarily render the incident immaterial. The Staff reiterated the adopting release for Item 1.05, which states that a registrant "should take into consideration all relevant facts and circumstances, which may involve consideration of both quantitative and qualitative factors" in determining whether a cybersecurity incident is material.[2] The Staff also notes that if the registrant has an insurance policy covering cybersecurity incidents, its materiality determination should also consider whether an insurer's reimbursement of a ransomware payment may affect the availability or cost of the insurance policy in the future.

- **Question 104B.08**: Whether the size of a ransomware payment by itself is indicative of the materiality of a ransomware attack.

  The Staff notes that the size of the ransomware payment is just one of the facts that should be considered to determine if the ransomware attack is a material cybersecurity incident. For example, the size of the ransomware payment may not be indicative of the reputational harm the registrant experiences as a result of an attack, or of other qualitative factors that may have a material effect on the registrant. The Staff reminds registrants that in its adopting release, the SEC declined to adopt "a quantifiable trigger for Item 1.05 because some cybersecurity incidents may be material yet not cross a particular financial threshold."[3]

- **Question 104B.09**: Whether a registrant is required to disclose in Item 1.05 a series of cybersecurity incidents involving ransomware attacks over time if each incident is individually immaterial.

  The Staff notes that a series of ransomware attacks over time may be reportable under Item 1.05 depending on the facts and circumstances around the incidents. The Staff reiterates that the materiality of a series of related incidents should be assessed in the aggregate. While the Staff does not offer any additional guidance regarding unrelated attacks, it quotes the adopting release to clarify that attacks involving "the same malicious actor engag[ing] in a number of smaller but continuous cyberattacks related in time and form against the same company" or "a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially" may be material when taken collectively, even if each attack by itself is immaterial.[4]

The full text of the new C&DIs can be found **here**.

2 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, Release Nos. 33-11216; 34-97989 (July 26, 2023) [88 FR 51896, 51917 (Aug. 4, 2023).

3 *Id.*

4 *Id.*

Activism Update

SEC Settles Charges Against Investment Advisors in Connection with Misleading Disclosures Related to Collaborations with Activist Short Publishers

On June 11, 2024, the SEC **announced** that it had settled charges against Anson Funds Management, LP, a registered investment advisor, and Anson Advisors, Inc., an exempt reporting advisor, related to a concealed collaboration with activist short publishers to issue short reports on target securities. While the release of negative information by activist short sellers is generally not illegal under U.S. law, the charges against Anson may signal an increased focus on deceptive methods of short activism.

Short attacks are carefully planned and coordinated attacks by an activist short seller that involve taking a large short position in a company then attempting to drive the share price down by the release of negative information. This information can be released in a variety of ways, including via a research paper, media placements or on message boards and blogs. The short attacker intends to drive down the target company's share price, thereby creating a return on its short position.

Background on the Case: Anson Funds and Anson Advisors (collectively, "Anson") were co-investment advisors in Anson Investment Master Fund ("AIMF"), a private pooled investment vehicle. Anson Fund and Anson Advisors worked together to fix AIMF's strategy, manage risks, create marketing materials and communicate with investors. At the center of the SEC's allegations is AIMF's private placement memorandum, which Anson sent to investors, describing its investment strategy for short positions as combing the market for companies where Anson believed improvements to underlying business prospects did not justify substantial short-term stock price appreciation, and examining industry trends to identify companies that they expected to experience similar stock price declines so that they could take and hold a short position until prices decreased in line with the industry-wide decline.[5] The SEC alleged, however, that AIMF omitted in its private placement memorandum another material component of its short position investment strategy, which effectively misled investors. Specifically, the SEC alleged that between 2018 and 2023, Anson collaborated with activist short publishers who issued reports with bearish information about certain target securities, and would sometimes share such short reports with Anson prior to making them public, with AIMP securing a short position prior to the release of the report. As a result of the report, the price of the target securities would often drop and AIMF would profit by covering its short position. In exchange, Anson agreed to pay the publishers a percentage of the profits AIMF received from trading in the target securities around the time the short report was published. Sometimes these arrangements were agreed to in formal consulting agreements, and at other times they were more informal arrangements in which Anson and the short publishers would exchange content and research.

The SEC alleged that these agreements and payments to short publishers were material information to investors and that the omission of this information in the AIMF private placement memorandum made it materially misleading. In addition, the SEC alleged that Anson Funds inaccurately recorded its payments to the short publishers by recording them as payments to third-party intermediaries for "research services" when they were really trading profits paid to the publishers in violation of their compliance policies and procedures.

Outcome: Anson was found to have willfully violated the Investment Advisers Act of 1940 (the "IAA"), which prohibits an investment advisor to a pooled investment vehicle from making "any untrue statement of a material fact or to omit to state a material fact necessary to make the statements made not misleading, or … otherwise engag[ing] in any act, practice, or course of business that is fraudulent, deceptive, or manipulative with respect to any investor or prospective investor in the pooled investment vehicle."[6] In addition, Anson Funds was found to have violated additional portions of the IAA for failing to "adopt and implement written policies and procedures reasonably designed to prevent violations of the Advisers Act and the rules thereunder" and for failing to "keep true, accurate and current books and records in specified categories."[7]

---

5 See *In the Matter of Anson Funds Management, LP and Anson Advisors, Inc., Release No. 6622 (June 11, 2024), https://www.sec.gov/files/litigation/admin/2024/ia-6622.pdf .*

6 *Id. at para 25.*

7 *Id. at para 26 - 27.*

Key Takeaways: While the SEC charges focused on material omissions in AIMF's private placement memorandum and failure to accurately record payments made to activist short publishers, the question of whether Anson could be charged for its underlying conduct—its collaboration with activist short publishers to exchange information for a piece of the short profits—remains open. Section 206(4) of the IAA prohibits investment advisors from engaging generally in "any act, practice, or course of business which is fraudulent, deceptive, or manipulative," leaving the door open for enforcement actions against schemes like the one Anson employed.[8]

Other Updates

First Federal Court Issues Order on Preliminary Injunction On FTC's Noncompete Ban

On July 3, 2024, the Northern District of Texas issued a ruling regarding the Federal Trade Commission's Non-Compete Clause Rule (the "Rule"), which was set to prohibit most employee non-compete agreements. The Court granted plaintiffs' motion for a preliminary injunction and postponed the effective date of the Rule as applied to the plaintiffs. The Court stated that it intends to rule on the ultimate merits of the action on or before August 30, 2024. For more information, please see our **client alert**.

A New Stock Exchange In Texas?

News that two large investor funds were aiming to launch a new electronic stock exchange headquartered in Dallas, Texas has been met with optimism, skepticism and questions about what the upstart might mean for established exchanges. The Texas Stock Exchange ("TXSE")—having raised $120 million from investment firms and individuals—plans to file for registration with the SEC later this year, with trading expected to begin in 2025 and listings kicking off the following year. The effort follows similar recent attempts by IEX, the Long-Term Stock Exchange, MEMX and others that have largely left the dominance of the NYSE and Nasdaq intact. The TXSE is presenting itself as a more "CEO-friendly" alternative exchange and comes at a time when its primary competitors are facing increasing commentary with respect to high compliance and trading costs. The proposal follows a series of developments aimed at presenting Texas as a business-friendly jurisdiction. The state is tied for second as the state with the most Fortune 500 companies, recently established the Texas Business Courts to compete with the Delaware Chancery Court and has been the site of high-profile business expansions and relocations in recent years, in addition to having favorable regulatory and tax policies. While the TXSE appears to be focused on becoming more of a regional exchange in the Southeast, supporters point to its potential role as a moderating force in the current duopoly, one that could improve efficiencies and benefit investors and registrants. Others wonder whether it can meaningfully compete given the entrenchment of current exchanges.

Despite strong support and a compelling business case, the TXSE faces significant hurdles and would need to compete with the deep-rooted infrastructure, extensive global reach, reputation and significant liquidity advantages that the NYSE and Nasdaq have over any new exchange. As all exchanges are overseen by the SEC, the TXSE must seek and receive approval from the SEC to operate as an exchange and, going forward, must abide by SEC regulations. Similarly, all exchange rules are subject to SEC approval to ensure that they are consistent with the Exchange Act, potentially limiting the extent to which rules can differ between exchanges. Following regulatory approval, the exchange will need to establish the infrastructure necessary to function effectively. While the TXSE will operate as an electronic, digital-only exchange, eliminating the need for a trading floor, and only anticipates requiring 100 or so employees at its headquarters, it will need to ensure access to the type of advanced technological systems needed to handle high-volume trading, settlement and cybersecurity for market participants.

Most challenging, however, will be wresting away listings and trading volume from the NYSE and Nasdaq. Ultimately, it will need to attract sufficient listings and trading volume to grow to become a credible destination for public companies, maintain liquidity and earn fees to cover its ongoing operational costs. The TXSE plans to compete for listings from the growing southeastern quadrant of the U.S. and to permit dual listings, such that a registrant need not only list on the TXSE, easing some trepidation that may otherwise accompany listing only on a new exchange.

Key Takeaways: What this will mean for the NYSE and Nasdaq depends on whether the TXSE can overcome hurdles that others have struggled to overcome. Other regional exchanges—including the Chicago Stock Exchange and Philadelphia Stock Exchange—have combined with the NYSE and Nasdaq, resulting in significant market concentration. The measure of the TXSE's success will be whether it can garner a meaningful number of listings and sufficient trading volume to impact the established exchanges. The success of the TXSE would reflect a trend towards greater decentralization in financial markets and business operations, emphasizing the importance of regional economic hubs outside of traditional financial centers.

8 Investment Advisers Act of 1940, 15 U.S. Code § 80b–6.

California's Workplace Violence Prevention Law Takes Effect

On September 30, 2023, Governor Gavin Newsom signed Senate Bill 553 (the "Workplace Violence Prevention Act"), which requires most California employers to develop and implement a comprehensive Workplace Violence Prevention Plan. The Workplace Violence Prevention Act also has three independent, though related, requirements: (1) regular workplace violence training, (2) the creation and maintenance of a workplace violence log and (3) recordkeeping.

Most California companies, subject to limited exemptions, must begin complying with each of the Workplace Violence Prevention Act requirements starting July 1, 2024. For more information on the requirements of the Workplace Violence Prevention Act, please see our **client alert**.

Litigation Update

The Supreme Court Grants Cert to Consider Questions Related to Risk Disclosures

On June 10, 2024, the U.S. Supreme Court granted a petition for certiorari in *Facebook, Inc. v. Amalgamated Bank*, No. 23-980, in which the Court will consider the question of whether "risk disclosures [are] false or misleading when they do not disclose that a risk has materialized in the past, even if that past event presents no known risk of ongoing or future business harm."[9]

Background: The appeal arises out of a private securities-fraud class action filed against Facebook (now Meta) relating to Cambridge Analytica's misuse of Facebook user data. In December 2015, a British newspaper reported that a professor had sold data he had acquired through a personality quiz app on Facebook to Cambridge Analytica, which used the data to create profiles of U.S. voters to support Ted Cruz's presidential campaign.[10] The professor and Cambridge Analytica told Facebook that they had purged all Facebook data from their systems.[11] These news reports had no effect on Facebook's stock price.[12]

In March 2018, news reports disclosed that Cambridge Analytica had in fact retained Facebook user data and used it in support of the Trump presidential campaign.[13] In contrast to the 2015 news reports, the 2018 news reports purportedly caused an 18% drop in the price of Facebook shares.[14]

Facebook shareholders filed an action in the Northern District of California asserting claims under Section 10(b) of the Securities Exchange Act of 1934, alleging that certain statements in Facebook's discussion of "risk factors" in its 2016 Form 10-K filing (issued after the December 2015 news reports but before the March 2018 news reports) were false.[15] The risk factors included warnings that "[s]ecurity breaches and improper access to or disclosure of our data or user data, or other hacking and phishing attacks on our systems, could harm our reputation and adversely affect our business," but did not mention the disclosure of Facebook user data to Cambridge Analytica.[16] Plaintiffs alleged that these disclosures were false because they framed the risk of data misuse as hypothetical, when such risk had already come to pass by the time of the 2016 Form 10-K.[17] Facebook argued that while it knew that the risk had materialized in the past, it had no reason to know at the time of the disclosure that there was a risk of ongoing or future harm to its business.[18]

While the district court dismissed plaintiffs' claims, a divided panel of the Ninth Circuit reversed the district court's dismissal in part, holding that Facebook's disclosures "represented the risk of improper access to or disclosure of Facebook user data as purely hypothetical when that exact risk had already transpired."[19] One member of the panel dissented, finding that plaintiffs had not "sufficiently alleged that Facebook knew its reputation and business were already harmed at the time of the filing of the 10-K."[20]

---

9 Cert. Pet. at i.

10 *Id.* at 6-7.

11 *Id.* at 7.

12 *Id.*

13 *Id.*

14 *Id.* at 8.

15 *Id.* at 9-10.

16 *Id.* at 10.

17 *Id.*

18 *Id.* at 17.

19 *In re Facebook, Inc. Securities Litigation*, 84 F.4th 844, 859 (9th Cir. 2023).

20 *Id.* at 870 (emphasis in original).

In the same certiorari petition, Facebook also sought review of the Ninth Circuit's decision regarding whether Rule 8 or Rule 9(b) of the Federal Rules of Civil Procedure supply the proper pleading standard for the element of loss causation in a private securities fraud action,[21] but the Supreme Court did not grant certiorari for that question.

Key Takeaways: This case could resolve the important question of whether a public company must disclose past events that demonstrate that certain risks have previously materialized. If the Supreme Court upholds the Ninth Circuit's decision, public companies may be required to disclose past risks that have come to pass, even if the company has no reason to suspect that those prior events pose an ongoing or future risk of harm to the business.

The Supreme Court Grants Cert to Consider Questions Related to Pleading Standards for Securities Fraud Class Actions Under the PSLRA

On June 17, 2024, the U.S. Supreme Court granted a petition for certiorari in *NVIDIA Corp., et al. v. E. Ohman J:or Fonder AB, et al.*, in which the Court will consider two important questions relating to the pleading standards for securities fraud class actions under the Private Securities Litigation Reform Act of 1995 ("PSLRA").[22] The first question is "[w]hether plaintiffs seeking to allege scienter under the PSLRA based on allegations about internal company documents must plead with particularity the contents of those documents."[23] The second question is "[w] hether plaintiffs can satisfy the PSLRA's falsity requirement by relying on an expert opinion to substitute for particularized allegations of fact."[24]

The case arises out of a private securities fraud class action filed against NVIDIA and its CEO. NVIDIA sells graphics processing units ("GPUs"), which accelerate computation by using parallel processing.[25] While NVIDIA's "GeForce" branded GPUs are designed and marketed for video gaming, they can also be used for cryptocurrency mining.[26] NVIDIA also developed and sold a new GPU designed and marketed specifically for cryptocurrency mining called "Crypto SKU."[27] While GeForce GPUs can be used for both video gaming and crypto mining, Crypto SKU can only be used for crypto mining.[28] NVIDIA reported revenue from GeForce GPUs in its "gaming" segment, while it reported revenue from Crypto SKU in a different segment.[29] In late 2018, after a record run up in sales, NVIDIA's sales of GeForce GPUs dropped, allegedly causing a decrease in NVIDIA's stock price.[30] After the stock drop, NVIDIA shareholders filed a putative class action lawsuit under Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5(b) in the United States District Court for the Northern District of California, alleging that NVIDIA and its CEO knowingly understated the extent to which NVIDIA's gaming segment revenues were driven by sales of GeForce GPUs to cryptocurrency miners, as opposed to gamers.[31]

To plead a claim under Section 10(b), plaintiffs must allege (among other things) "a material misrepresentation or omission by the defendant" and "scienter."[32] Pursuant to the PSLRA, which imposes "exacting pleading requirements" for private securities fraud actions, plaintiffs must "state with particularity. . . the facts constituting the alleged violation" as well as "'facts giving rise to a strong inference that the defendant acted with the required state of mind.'"[33]

In support of their scienter allegations, plaintiffs cited statements from former NVIDIA employees that stated that NVIDIA created internal reports analyzing GPU sales and usage data, without describing the contents of any such reports.[34]

---

21 Cert. Pet. at i.

22 *NVIDIA Corp., et al. v. E. Ohman J:or Fonder AB, et al.*, No. 23-970.

23 Cert. Pet. at i.

24 *Id.*

25 *Id.* at 8.

26 *Id.*

27 *Id.*

28 *Id.*

29 *Id.*

30 *Id.* at 9.

31 *Id.* at 9-10.

32 *Id.* at 7 (quoting *Stoneridge Inv. Partners, LLC v. Scientific-Atlanta, Inc.*, 552 U.S. 148, 157 (2008)).

33 *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 311, 313-314 (2007) (quoting 15 U.S.C. § 78u-4(b)(2)).

34 Cert. Pet. at 11.

In support of their falsity allegations, plaintiffs' complaint relied on an expert opinion purporting to show that most of NVIDIA's gaming revenues were attributable to cryptocurrency miners' purchases of GeForce GPUs.[35] The United States District Court for the Northern District of California twice dismissed plaintiffs' claims for failure to adequately plead a cause of action under Section 10(b),[36] but a divided panel of the Ninth Circuit reversed with respect to the claims against NVIDIA and NVIDIA's CEO.[37]

The first question raised by the petition is what a plaintiff must plead regarding internal company documents to demonstrate scienter in a securities action. One way in which plaintiffs often allege scienter is to claim that executives reviewed contemporaneous internal documents contradicting their public statements.[38] On how much a complaint must allege regarding such documents, there is a circuit split: while the Second, Third, Fifth, Seventh and Tenth Circuits require plaintiffs to allege with particularity the actual contents of such documents, the First and Ninth Circuits (in the instant case) would allow plaintiffs to proceed past a motion to dismiss based on allegations speculating as to what those documents might have said.[39]

The second question raised by the petition is the extent to which a plaintiff can plead falsity by relying on the opinion of an expert. In this case, plaintiffs hired an expert to provide an opinion on how much of much of NVIDIA's gaming revenues were attributable to cryptocurrency miners purchasing GeForce GPU.[40] This opinion was based on various assumptions that were challenged as unsupported by NVIDIA.[41] While the Second and Fifth Circuits have held that such expert opinions can only be used to "bolster" a complaint, and not replace particularized factual allegations in support of the falsity of an alleged misstatement, the Ninth Circuit's decision below relied directly on plaintiffs' expert opinion in determining the question of whether defendant's statements were adequately alleged to be false.[42]

This case will resolve two important circuit splits concerning the pleading requirements for securities fraud class actions. In particular, as the petition emphasized, resolving the splits between the Second and Ninth Circuits on these two issues is important, because those two circuits account for the significant majority of private securities actions nationwide.[43]

◇ ◇ ◇

35 *Id.* at 10-11.

36 *Iron Workers Loc. 580 Joint Funds v. NVIDIA Corp.*, 522 F. Supp. 3d 660, 665 (N.D. Cal. 2021).

37 *E. Ohman J:or Fonder AB v. NVIDIA Corp.*, 81 F.4th 918, 924 (9th Cir. 2023).

38 Cert. Pet. at 14-15.

39 *Id.* at 13-14.

40 *Id.* at 10.

41 *Id.* at 10-11.

42 *Id.* at 5.

43 *Id.*

About Paul Hastings

With widely recognized elite teams in finance, mergers & acquisitions, private equity, restructuring and special situations, litigation, employment, and real estate, Paul Hastings is a premier law firm providing intellectual capital and superior execution globally to the world's leading investment banks, asset managers, and corporations.