**UNITED STATES DISTRICT COURT**
**FOR THE SOUTHERN DISTRICT OF NEW YORK**

| | | |
|---|---|---|
| SECURITIES AND EXCHANGE COMMISSION,<br><br>*Plaintiff*,<br>v.<br><br>SOLARWINDS CORP. and TIMOTHY G. BROWN,<br><br>*Defendants*. | : | Case No.: 1:23-CV-09518 (PAE) |

**BRIEF OF AMICI CURIAE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA AND BUSINESS ROUNDTABLE IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS**

Nicole Friedlander
SULLIVAN & CROMWELL LLP
125 Broad Street
New York, New York 10004
Telephone: (212) 558-4000
Facsimile: (212) 558-3588
friedlandern@sullcrom.com

Jeffrey B. Wall (*pro hac vice* pending)
SULLIVAN & CROMWELL LLP
1700 New York Avenue NW, Suite 700
Washington, DC 20006
Telephone: (202) 956-7500
Facsimile: (202) 293-6330
wallj@sullcrom.com

*Counsel for Amici Curiae*

February 2, 2024

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Page(s)**

**Cases**



**Statutes and Rules**

**Other Authorities**

## IDENTITY AND INTEREST OF AMICI CURIAE

The Chamber of Commerce of the United States of America is the world's largest business federation. The Chamber directly represents approximately 300,000 members and indirectly represents the interests of more than 3 million companies and professional organizations of every size, in every economic sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members by participating as an amicus curiae in cases, like this one, that raise issues of concern to the nation's business community.

Business Roundtable represents the chief executive officers (CEOs) of over 200 of America's leading companies. The CEO members lead U.S.-based companies that support one in four American jobs and almost a quarter of U.S. gross domestic product. Business Roundtable was founded on the belief that businesses should play an active and effective role in the formulation of public policy, and its members develop and advocate for policies to promote a thriving economy and expanded opportunity for all.

The Chamber and Business Roundtable have a significant interest in this case. The SEC's expansion of the internal-accounting-controls provision of the FPCA would enable it to charge any public company with a violation of the federal securities laws for failing to apply the company's own internal policies or even for being the victim of crime. The SEC has already asserted this power, far beyond what Congress intended, in non-litigated actions against other public companies, extracting large penalties. The SEC's interpretation creates profound uncertainty for the members of the Chamber and Business Roundtable because it suggests a standard that is virtually impossible to meet and discernible only in hindsight.[1]

[1] No party's counsel authored this brief in whole or in part; no party or party's counsel contributed money intended to fund the preparation or submission of this brief; and no person other

## INTRODUCTION

Congress adopted the Foreign Corrupt Practices Act of 1977 (FCPA) to combat the use of corporate funds to bribe foreign officials. To make it harder to conceal illicit payments, Congress through the FCPA added Section 13(b)(2)(B) to the Securities Exchange Act, requiring public companies to "devise and maintain a system of internal accounting controls." 15 U.S.C. § 78m(b)(2)(B). Those controls are meant to ensure that management authorizes "transactions" and "access to assets," and properly records and accounts for those transactions and assets, to enable the company to prepare its "financial statements in conformity with generally accepted accounting principles." 15 U.S.C. § 78m(b)(2)(B)(i)-(iv). As a textual matter, it could hardly be clearer that "accounting controls" are measures to ensure the reliability of financial reporting. And given the text, courts have consistently held that Section 13(b)(2)(B) covers *only* controls related to financial reporting, not all internal controls.

The text alone is dispositive, but the history should make the SEC blush. The SEC itself proposed the language that became the accounting-controls provision. It borrowed the language nearly verbatim from the American Institute of Certified Public Accountants' Statement on Auditing Standards 1 (SAS 1), which expressly stated that "accounting controls" are controls that have an "important bearing on the reliability of the financial statements." SAS 1, §§ 320.11-12. SAS 1 further explained that accounting controls are concerned with unauthorized "access to assets" only insofar as it creates *accounting* risk—that is, the risk that a company could be unaware of a loss of assets reported in its financial statements (primarily liquid assets such as cash, securities, and inventory), and thus incorrectly account for the assets in its financial statements.

---

than the amici, their members, or their counsel contributed money that was intended to fund preparing or submitting the brief.

*See* SAS 1, §§ 320.42, 320.36, 320.15. Those settled meanings travelled with the language, and the SEC and Congress for decades described accounting controls, and their objective of reasonably ensuring that access to assets is authorized, solely by reference to financial reporting.

As if all of that were not enough, there is a parallel provision of Sarbanes-Oxley that requires "internal control[s] . . . for financial reporting," 15 U.S.C. § 7262(a)(1)—and the SEC has long said it interprets the two statutes *in pari materia*. The SEC has not defined "internal control[s] . . . for financial reporting" as all internal controls, or as all controls intended to protect anything a company owns. Rather, the SEC has defined that phrase only in the context of financial reporting risk. It requires companies to have controls that prevent or timely detect the unauthorized acquisition, use, or disposition of assets "that could have a material effect on the financial statements," 17 C.F.R. § 240.13a-15(f)(1)-(3)—and the SEC has made clear that is all Section 13(b)(2)(B)(iii) requires as well. Indeed, the SEC rejected reading Sarbanes-Oxley more broadly for reasons of text, workability, and cost that apply equally to Section 13(b)(2)(B). In short, all of the indicia of statutory meaning—text, history, case law, parallel provisions, and the SEC's own guidance—point in the same direction.

None of that, however, has stopped the SEC from gradually converting Section 13(b)(2)(B) into a general grant of corporate police power. Over time, and as this case shows, the SEC has invoked the provision to pursue substantial penalties against companies that allegedly failed to comply with controls that had nothing to do with the accuracy of their financial statements. Here, the SEC alleges that "shortcomings" in "SolarWinds' cybersecurity-related policies and procedures" enabled hackers to access SolarWinds's systems. ECF No. 1 (Compl.) ¶¶ 198, 200; *see id.* ¶¶ 194-200. But the SEC notably does not claim that those alleged failures posed any risk,

much less a material risk, to the reliability of the company's financial statements. Failing to prevent a trespass, whether in physical space or cyberspace, is not a violation of the FCPA.

Under the SEC's contrary reading, companies can be in violation of the federal securities laws for failing to apply a host of internal policies or even for being the victims of crime. In recent years, the SEC has challenged everything from stock buyback policies to airline flight routes. Its power grab has left companies in constant peril and uncertainty about how to design their internal control systems, because once "accounting controls" are no longer about accounting, virtually everything is fair game. This case is an excellent example. The SEC is not a cybersecurity enforcement agency—it is not remotely equipped to judge whether SolarWinds's systems were reasonably designed to repel an attack by a hostile nation-state with advanced cyber capabilities. Nor does it have the statutory directive to address this question: whatever the answer, it has nothing to do with the FCPA or Congress's desire to make it harder to conceal illicit payments. Because the SEC's Complaint does not point to SolarWinds's failure to design or maintain any "accounting controls," the Seventh and Eighth Claims for Relief should be dismissed.[2]

## I. THE SEC'S INTERPRETATION IS AT ODDS WITH THE EXCHANGE ACT'S TEXT, ITS HISTORY, AND THE AGENCY'S OWN GUIDANCE.

The text and legislative history of Section 13(b)(2)(B), as well as related SEC guidance and case law, demonstrate that the provision applies only to "internal *accounting* controls." 15 U.S.C. § 78m(b)(2)(B) (emphasis added). As the plain text indicates, those controls ensure the

[2] Although this brief focuses on the SEC's claims under Section 13(b)(2)(B), the Chamber and Business Roundtable also support the arguments of other *amici* about the perverse consequences of the SEC's action for companies' security. As those amici explain, the SEC's approach in this case will discourage candid communications by cybersecurity personnel about important cybersecurity matters, and expose companies to security risk to the extent the SEC purports to require disclosure of unremediated vulnerabilities.

reliability of a public company's financial reporting. Congress has never granted the SEC authority to regulate other aspects of a public company's larger internal-control framework.

### A. The Text Of Section 13(b)(2)(B) Refers Only To Internal "Accounting" Controls, Not All Internal Controls.

Read as a whole, the text of Section 13(b)(2)(B) could not be clearer. It requires companies to "devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances" that company personnel are not engaging in unauthorized or unreported financial transactions that could affect the reliability of companies' financial statements. 15 U.S.C. § 78m(b)(2)(B). On its face, the provision refers only to "accounting" controls, not operational or compliance controls, or internal controls more broadly. *Id.* "Internal accounting control is, generally speaking, only one aspect of a company's total control system; in order to maintain accountability for the disposition of its assets, a business must attempt to make it difficult for its assets to be misappropriated." *SEC* v. *World-Wide Coin Invs., Ltd.*, 567 F. Supp. 724, 750 (N.D. Ga. 1983).

Congress also set forth the objectives that a company's accounting controls must reasonably ensure: first, that "transactions are executed in accordance with management's general or specific authorization," 15 U.S.C. § 78m(b)(2)(B)(i); second, that "transactions are recorded as necessary" "to permit preparation of financial statements in conformity with generally accepted accounting principles" and "to maintain accountability for assets," *id.* § 78m(b)(2)(B)(ii)(I)-(II); third, that "access to assets is permitted only in accordance with management's general or specific authorization," *id.* § 78m(b)(2)(B)(iii); and fourth, that "the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences," *id.* § 78m(b)(2)(B)(iv).

Every bit of that text indicates that Congress was concerned solely with the reliability of financial reporting. To prevent the concealment of bribes, Section 13(b)(2)(B) requires that management authorize "*transactions*" and "access to *assets*"; that transactions be documented in "*financial statements* in conformity with generally accepted *accounting principles*" to maintain "*accountability* for *assets*"; and that "the *recorded accountability* for *assets* is compared with the existing assets" periodically to reconcile the company's books. 15 U.S.C. § 78m(b)(2)(B)(i)-(iv) (emphases added). As the text shows, companies are required to authorize transactions and "access to assets" as part of a process (including timely recording, accurate accounting, and periodic reconciliation) that helps ensure the reliability of their financial statements. 15 U.S.C. § 78m(b)(2)(B). Thus, Section 13(b)(2)(B) is a tailored provision that serves Congress's specific objective of deterring bribery, and not a general security measure.

Although the provision's text is dispositive, its heading, which uses the phrase "internal accounting," 15 U.S.C. § 78m(b), also indicates that Congress was concerned with only one aspect of a company's internal-control system—its accounting controls. *See Yates* v. *United States*, 574 U.S. 528, 552 (2015) (Alito, J., concurring) (statutory heading is "especially valuable" evidence of meaning when "it reinforces what the text[] independently suggest[s]"). The same focus is clear from the title's reference to Section 13(b)(2)(B)'s companion provision requiring companies to maintain books and records that reasonably reflect their "transactions and dispositions of . . . assets." 15 U.S.C. § 78m(b)(2)(A). The two provisions work together to accomplish Congress's aim of ensuring reliable financial reporting.

In light of Section 13(b)(2)(B)'s text, courts, including in this District, have consistently held that the provision covers only controls related to financial reporting. In *In re Elan Corp. Securities Litigation*, for example, the plaintiffs alleged that the defendants had violated Section

13(b)(2)(B) because the company's internal controls did not ensure that unfavorable clinical-trial results were timely reported to the FDA. 543 F. Supp. 2d 187, 222-223 (S.D.N.Y. 2008) (Holwell, J.). The court dismissed the claim, stating that the purpose of Section 13(b)(2)(B) is "to ensure accurate accounting and financial reporting," and that the plaintiffs had failed to allege "any misstatement or omission regarding financial or accounting information." *Id.* at 223; *see SEC* v. *Rio Tinto plc*, 2019 WL 1244933, at *19 (S.D.N.Y. Mar. 18, 2019) (Torres, J.) (dismissing Section 13(b)(2)(B) claim because, in claiming the company's controllers submitted false documents to auditors, SEC failed to allege sufficient facts about the accounting controls that were supposedly violated); *SEC* v. *Felton*, 2021 WL 2376722, at *12 (N.D. Tex. June 10, 2021) (dismissing Section 13(b)(2)(B) claim where "the SEC d[id] not identify a single internal control that govern[ed] the handling of sales, inventory, exchanges, returns, recognition of revenue, etc.") (internal quotation marks omitted); *SEC* v. *Patel*, 2009 WL 3151143, at *26-27 (D.N.H. Sept. 30, 2009) (dismissing Section 13(b)(2)(B) claim where SEC's allegations "sa[id] nothing about manual or automated reviews of records, methods to record transactions, reconciliation of accounting entries, or anything else that might remotely qualify as an internal accounting control") (citation omitted); *cf. In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1226-1227 (N.D. Ga. 2019) (dismissing claim that allegedly deficient cybersecurity rendered false a company's certification that it had effective internal control over financial reporting because "[a] reasonable investor would not take assurances of internal controls to detect improprieties in accounting and bookkeeping to guarantee that there were systems in place to deal with cybersecurity breaches").[3]

[3] Even if there were any doubt about the meaning of "internal accounting controls," the rule of lenity resolves it. Violations of Section 13(b)(2)(B) are subject to both civil and criminal penalties, which requires resolving any ambiguity in favor of the narrower meaning that "internal accounting controls" are only those controls that directly bear on companies' accounting and financial reporting. *See Leocal* v. *Ashcroft*, 543 U.S. 1, 11-12 n.8 (2004).

Thus, both the statute's text and the weight of authority treat "accounting controls" as a discrete set of controls that reasonably ensure the reliability of a company's financial statements.

**B. The History Of Section 13(b)(2)(B) Confirms Its Plain Text.**

Congress enacted the FCPA in response to a series of foreign bribery scandals. To make it harder to conceal bribes, Congress required companies to "maintain strict accounting standards and management control over their assets." S. Rep. No. 95-114, at 2 (1977); *see* Presidential Statement on Signing the [FCPA] into Law, 2 Pub. Papers 2157 (Dec. 20, 1977) (FCPA requires public companies to "establish accounting controls to prevent the use of 'off-the-books' devices, which have been used to disguise corporate bribes in the past.").

The SEC knows this. In its report to Congress urging adoption of the FCPA, the Commission itself proposed the language that was lifted into Section 13(b)(2)(B). *See* SEC, 94th Cong., *Report on Questionable and Illegal Corporate Payments and Practices* 63-65 (Comm. Print 1976) (SEC Report). The SEC told Congress

> that any legislation should require management to establish and maintain its own system of internal accounting controls designed to provide reasonable assurances that corporate transactions are . . . [authorized and] are properly reflected on the corporation's books and records in such a manner as to permit the preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements.

*Id*. at 58-59. The SEC thus described the provision purely in financial-reporting terms.

What is more, the SEC had borrowed its proposed language essentially verbatim from SAS 1, which defined "accounting controls" and their four objectives. *See* Am. Inst. of Certified Pub. Accts., Codification of Auditing Standards & Procs., Statement on Auditing Standards No. 1, § 320.28 (1973). The SEC told Congress that SAS 1 was the "authoritative accounting literature," and the Senate Report that accompanied the FCPA says the same thing. *See* SEC Report at 59; S. Rep. No. 95-114, at 8 (1977). Because Congress essentially adopted SAS 1's terminology and

objectives, and did so on the SEC's recommendation, it is both helpful and revealing to look at how SAS 1 defined accounting controls, which focused solely on ensuring the reliability of financial statements.

SAS 1 identified "accounting controls" as only a subset of companies' internal controls, and defined them as "the plan of organization and the procedures and records that are concerned with the safeguarding of assets and the reliability of financial records [for external reporting]." SAS 1, § 320.28. Importantly, SAS 1 clarified that "safeguarding of assets" should *not* be interpreted broadly as "a means of protection against something undesirable," since that "broad definition" could conceivably cover every record and process entering into every decision a company makes about how to earn or spend money. *Id*. § 320.14-15, 320.19. Instead, the term "refer[s] *only to protection against loss* arising from intentional and unintentional errors in processing transactions and handling the related assets." *Id.* § 320.15 (emphasis added).[4] SAS 1 provided examples of such "loss," including "understatement of sales," "overpayment to vendors or employees," or "physical loss of assets such as cash, securities, or inventory." *Id*. Each example involves an asset reported on a company's balance sheet (*i.e.*, money, securities and inventory), as opposed to an asset in the colloquial sense of anything that someone owns or possesses.[5]

---

[4] The AICPA has recharacterized the components of companies' overall internal control frameworks since AS 1 was published in 1973. While SAS 1 divided them into "accounting controls" and "administrative controls," the AICPA currently identifies three categories of internal controls: financial reporting, operational, and legal and compliance controls. *Compare* SAS 1, § 310.10, *with* Am. Inst. of Certified Pub. Accts., Codification of Auditing Standards & Procs, Statement on Auditing Standards No. 145 § 12 (2021) (defining "[s]ystem of internal control"). Financial reporting controls include the controls required by Section 13(b)(2)(B), as the SEC itself has made clear. *See infra*, pp. 11-13.

[5] *Compare* Elements of Financial Statements, Statement of Fin. Acct. Concepts No. 8, *Elements of Financial Statements* ¶ E16 (Fin. Acct. Standards Bd. 2021) ("An asset is a present right of an entity to an economic benefit"), *and* Fin. Acct. Standards Bd., Acct. Standards Codification §§ 210-10-05-2, 210-10-05-5, https://asc.fasb.org/210/showallinonepage (Fin. Acct.

Based on its definition of "accounting controls," SAS 1 proposed the four objectives of a system of accounting controls that Congress codified as Section 13(b)(2)(B)(i)-(iv). *See id.* § 320.28. Those objectives—and their corresponding statutory subsections in the Exchange Act—are collectively meant to ensure that transactions and assets are authorized and recorded accurately to enable companies to prepare financial statements in accordance with generally accepted accounting principles. Specifically with respect to assets, SAS 1 focused solely on the risk that unauthorized access could cause inaccurate *accounting* for assets. For example, SAS 1 explained that timely recording of transactions would help "to maintain accountability for assets such as cash, securities, and others that are susceptible to loss from errors or irregularities." *Id.* § 320.40. SAS 1 noted that "anyone who . . . has access to assets ordinarily is in a position to perpetrate errors or irregularities" in financial statements, thus directly linking the access to assets with the ability to cause the misreporting of those assets in financial statements. *Id*. at § 320.36. SAS 1 further explained that in determining who was authorized to access assets, companies should consider "the nature of the assets and the related susceptibility to loss through errors and irregularities," again directly linking these two concepts. *Id*. at § 320.42.

The SEC even told Congress that the benefit of adopting SAS 1 was that it would be readily understood by auditors, who are responsible for auditing financial statements. *See* SEC Report at 59. Congress had the same understanding. For example, under the heading "[a]ccurate accounting," the Senate Report explains that the FCPA "strengthen[s] . . . the reliability of the *audit process* which constitute[s] the foundations of our system of corporate disclosure." S. Rep.

---

Standards Bd.) (explaining that assets are shown on the balance sheet), *with Assets, Merriam-Webster Dictionary*, https://www.merriam-webster.com/dictionary/assets (last visited Feb. 2, 2024) (noting additional, colloquial meanings of "assets" including any "item of value owned," any "advantage or resource" (*e.g.*, "His wit was his chief asset."), or something used to "defeat an enemy" such as military equipment).

No. 95-114, at 7 (1977) (emphasis added). The Senate Report further describes Section 13(b)(2)(B) as a means to support the SEC's "current program for accurate accounting," and says that the accounting profession's expertise will be necessary to assess companies' accounting controls. *Id.* at 7-8. There is no mention of Section 13(b)(2)(B) in the legislative record as anything other than a measure to ensure reliable financial reporting.

### C. The SEC's Own Guidance Shows That Internal Accounting Controls Address Material Financial-Reporting Risks.

Twenty-five years after passing the FCPA, and following a series of accounting scandals, Congress enacted Sarbanes-Oxley to further enhance the reliability of public companies' financial reporting. Under Section 404 of Sarbanes-Oxley and the SEC's implementing rule, management must address in the company's annual report the effectiveness of the company's "internal control over financial reporting." 15 U.S.C. § 7262(a)(1); 17 C.F.R. § 240.13a-15 (Rule 13a-15).

Critically, when the SEC promulgated Rule 13a-15 under Sarbanes-Oxley, it explained that its definition of "internal control over financial reporting" "is consistent with the description of internal accounting controls in Exchange Act Section 13(b)(2)(B)." Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, 68 Fed. Reg. 36636, 36640, Release No. 33-8238, Exchange Act Release No. 34-47986 (June 5, 2003) (Adopting Release). The SEC explained why it was important for Rule 13a-15's requirements to subsume those of Section 13(b)(2)(B): the U.S. General Accounting Office had previously noted that readers of companies' annual reports would reasonably assume that if a company reported that its financial-reporting controls were effective, the company was in compliance with the FCPA. *Id.* at 36641. Thus, the SEC made clear that the controls for "internal control over financial reporting" under Sarbanes-Oxley include the accounting controls required by the Exchange Act.

At the same time, the SEC defined "internal control over financial reporting" to mean controls that reasonably ensure "the reliability of a company's financial reporting," including that transactions and dispositions of assets are accurately recorded; that financial statements are prepared in accordance with generally accepted accounting principles; and that unauthorized use or diversion of assets is prevented or timely detected if it could have a material effect on the company's financial statements. *See* 17 C.F.R. § 240.13a-15(f)(1)-(3).

For assets in particular, Rule 13a-15(f)(3) under Sarbanes-Oxley requires controls that reasonably ensure the "prevention or timely detection of unauthorized acquisition, use or disposition of [an] issuer's assets *that could have a material effect on the [company's] financial statements*." 17 C.F.R. § 240.13a-15(f)(3) (emphasis added). The SEC's Adopting Release makes clear that this requirement subsumes the need under the Exchange Act for controls that reasonably ensure against unauthorized "access to assets." *See* Adopting Release at 36639-36640. In other words, the ultimate question under both Sarbanes-Oxley and the Exchange Act is whether the control prevents a misstatement of assets that could materially undermine the reliability of the company's financial statements. That is what marks an internal control as an *accounting* control.

All of that would be damning enough, but in interpreting Sarbanes-Oxley, the SEC expressly rejected a "considerably broader definition" of "internal control over financial reporting" that would capture non-accounting controls, including those "internal control objectives associated with enterprise risk management and corporate governance." *Id.* The Commission took that approach for "a variety of reasons," including that Section 404 of Sarbanes-Oxley refers only to "the element of internal control that relates to financial reporting" and accountants "traditionally have not been responsible for reviewing, testing, or attesting to an assessment by management of internal controls that are outside the boundary of financial reporting." *Id.* The SEC also reasoned

that "even the more limited definition related to financial reporting . . . will impose substantial burden and costs on companies." *Id.* at 36639. In fact, the SEC found the compliance burden was so substantial that it was necessary to further constrict the definition of "internal control over financial reporting" to only those financial reporting controls "*that could have a material effect on the financial statements*." *Id.* at 36640 (emphasis added).

Over the decades since the passage of Sarbanes-Oxley, companies have designed, implemented, assessed, and attested to the effectiveness of their internal control over financial reporting in accordance with the SEC's Rule 13a-15 and interpretive guidance. In particular, as companies' financial statements have increasingly relied on accounting software applications and other automated processes (as opposed to manual processes such as recording transactions by hand), companies have included among the suite of controls within their frameworks for internal control over financial reporting a discrete set of "IT general controls"—for instance, controls over applications that automate the flow of transactions into their financial reporting and thus could materially affect them. *See* Public Company Accounting Oversight Board (PCAOB), AS 2201: *An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements*, § 2201.27. The SEC, which oversees the PCAOB, has approved precisely that practice. "Specifically, it is *unnecessary* to evaluate IT general controls that primarily pertain to efficiency or effectiveness of a company's operations, but which are not relevant to addressing financial reporting risks." Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934, 72 Fed. Reg. 35324, 35328 nn.34-45, Release No. 33-8810, Exchange Act Release No. 34-55929 (June 20, 2007) (Interpretive Release) (examples of the only IT general controls relevant for internal control over financial reporting are "controls that perform automated

matching, error checking or edit checking functions," or "post[] correct balances to appropriate accounts or ledgers").

In accordance with the SEC and PCAOB guidance, the vast majority of companies' information-technology controls (including cybersecurity controls) do not fall within companies' frameworks for internal control over financial reporting because they have nothing to do with the reliability of financial reporting. Nor could they be included as a practical matter. Information technology controls are exceedingly complex, require specialized knowledge to assess, and change frequently, unlike accounting standards. While undoubtedly important, these controls are simply not subject to wholesale assessment by accounting professionals, who lack the relevant expertise to make such judgments. *See* Interpretive Release at 35328-35329.

The SEC's position in this case is thus inconsistent with the whole of its related interpretive regime under Sarbanes-Oxley and over 20 years of work by public companies and auditors to design, implement, assess, and audit the financial reporting controls that the regime requires. "A fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden . . . ." *FCC* v. *Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012); *see United States* v. *AMC Ent., Inc.*, 549 F.3d 760, 768 (9th Cir. 2008) ("[T]hose regulated by an administrative agency are entitled to know the rules by which the game will be played." (citation omitted); *Bynum* v. *U.S. Capitol Police Bd.*, 93 F. Supp. 2d 50, 59 (D.D.C. 2000) (finding unconstitutionally vague "an unwritten interpretation of [an agency] regulation" where "neither the statute *nor* the regulation expressly prohibit[ed]" the sanctioned conduct) (emphasis in original); *see also Karem* v. *Trump*, 960 F.3d 656, 666 (D.C. Cir. 2020) ("'[T]he principle of fair warning' requires that novel standards announced in adjudications 'must not be given

retroactive effect where they are unexpected and indefensible by reference to the law which had been expressed *prior to the conduct in issue*.'" (citation omitted) (emphasis in original) .

## II. THE SEC'S INTERPRETATION LEADS TO UNTENABLE CONSEQUENCES FOR ALL PUBLIC COMPANIES.

While Section 13(b)(2)(B) was enacted as part of "limited-purpose legislation" to combat foreign bribery, SEC Report at 57, in the SEC's hands, the provision has been abused as a roving mandate for the agency to penalize every aspect of companies' risk management. The SEC has found companies in violation of the federal securities laws simply for failing to apply their own internal policies, or processes the SEC deems appropriate. The SEC's power grab has left companies in constant peril and with profound uncertainty about how to design their internal-control systems.

### A. The SEC's Interpretation Makes the SEC a Cybersecurity Enforcement Agency and Converts Internal Policy Breaches Into Federal Securities Law Violations.

The SEC alleges that SolarWinds did not comply with certain of its own "cybersecurity-related policies and procedures," which resulted in a breach. Compl. ¶ 200. But the SEC is not a cybersecurity enforcement agency and is not equipped to assess cybersecurity, much less the complex array of cybersecurity matters that companies address in different industries and contexts. The Complaint demonstrates as much. The SEC suggests that the breach, which is widely viewed as the work of a hostile nation-state with advanced cyber capabilities, was simply the result of basic failures by SolarWinds. But any assessment of that claim would depend on highly technical facts not alleged in the Complaint, including (among other things) how the isolated alleged deficiencies operated in the context of any other controls employed by the company to prevent, detect and respond to an intrusion. Whatever the outcome of that analysis, the SEC is not capable of conducting it, and makes no claim to have done so.

Companies with cybersecurity programs routinely identify gaps in their compliance with their objectives, policies, and procedures, as well as vulnerabilities, many of which take time to address. It is the nature of the enterprise: new information technology introduces new risks, cyber threats evolve to evade defenses, and cybersecurity in turn has to adjust to mitigate those new risks and threats. Every company must prioritize remediation and enhancements based on the severity of the risk and the likelihood of harm. Put simply, if the SEC can charge a violation of Section 13(b)(2)(B) simply because a company has gaps in its cybersecurity controls or because it wants to second-guess the company's response, then the SEC can charge any company at any time.

Beyond cybersecurity, the SEC could penalize public companies whenever they violate their own internal policies. In recent years, the SEC has used Section 13(b)(2)(B) in exactly this way, penalizing companies that allegedly did not comply with or had deficient internal policies or processes unrelated to accounting. *See, e.g.*, *In re Andeavor, LLC*, Exchange Act Release No. 90208, 2020 WL 6112215, at *2 (Oct. 15, 2020) (finding that company violated Section 13(b)(2)(B) because its legal department followed too "abbreviated and informal" a process in approving a stock repurchase plan); *In re United Cont'l Holdings, Inc*., Exchange Act Release No. 79454, 2016 WL 7032725 (Dec. 2, 2016) (finding that airline violated Section 13(b)(2)(B) when its domestic flight route did not comply with its ethics policy).

The SEC has thus sought to vest itself with a vast and essentially unchecked power. For large entities like most public companies, it is exceedingly difficult, if not impossible, to ensure compliance with all policies, procedures, and controls at all times. By treating Section 13(b)(2)(B) as a grant of generalized monitoring authority, the SEC has attempted to position itself as a super-enforcer of corporate behavior well beyond the bounds of federal securities laws. The SEC's own Commissioners have objected to this overreach. *See* Statement of SEC Comm'rs Hester M. Peirce

and Elad L. Roisman – Andeavor LLC (Nov. 13, 2020), https://www.sec.gov/news/public-statement/peirce-roisman-andeavor-2020-11-13 (stating that "the Commission's resolution of this case . . . risks uprooting the core concept of 'internal accounting controls' from the language, statutory context, and history of Section 13(b)(2)(B)," and that it was improper to use Section 13(b)(2)(B), which "Congress confined" to a "limited scope," "to second-guess management[] . . . on matters that do not directly implicate the accuracy of a company's accounting and financial statements"); The SEC's Swiss Army Statute: Statement of SEC Comm'rs Hester M. Peirce and Mark T. Uyeda (Nov. 14, 2023) (criticizing "[t]he Commission's attempts to convert an internal accounting controls provision into an ever-unfolding utility tool that magically converts every corporate activity into something the Commission regulates"). And, of course, if the Commission has the back-end power to punish, then it has the front-end power to shape corporate behavior. *See id.* ("The Commission in recent years has taken to using . . . Section 13(b)(2)(B) as its own Swiss Army statute—a multi-use tool handy for compelling companies to adopt and adhere to policies and procedures that the Commission deems good corporate practice."). Congress did not hide such a broad and important power in an accounting-controls provision.

### B. The SEC's Interpretation Penalizes Companies For Being The Victims Of Crime.

Indeed, the implications of the SEC's overreach in this case are even greater than in *Andeavor*. The SEC makes the novel assertion that SolarWinds violated Section 13(b)(2)(B) because it failed to safeguard its information technology network environment, products, and source code from access by hackers. *See* Compl. ¶¶ 194-195. In divorcing "access to assets" in Section 13(b)(2)(B) from its accounting context, the SEC asserts the power to charge a violation based on any unauthorized interaction with any "important" tangible or intangible property of a

company, regardless of whether it affected or could have affected the company's financial statements, much less materially so.

Taken seriously, the SEC's reading of Section 13(b)(2)(B) means that companies would be exposed to liability when they are victims of crime. Whenever a hacker breaches a company system, or a thief steals product designs kept under lock and key, or an employee or outsider gains unauthorized access to company property of any kind, by definition the company either lacks sufficient controls or those controls fail. On the SEC's view, all of those crimes mean that the company may face civil or even criminal liability for being victimized. The only thing standing in the way of such liability is the SEC's grace—its discretionary decisions about which internal-control failures to pursue. None of this is what Congress intended when it required companies to have accounting controls to deter bribery.

### C. The SEC's Interpretation Injects Uncertainty Into Companies' Financial Reporting Systems.

As explained above, the SEC has traditionally interpreted "internal accounting controls" under the Exchange Act and "internal control over financial reporting" under Sarbanes-Oxley consistently. *See supra*, pp. 11-14. Its position here, however, divorces the two. The SEC now apparently believes that a company's internal accounting controls can be deficient whenever they allow unauthorized access to an "important" item of tangible or intangible property, even if that access has nothing to do with financial-reporting risks. Compl. ¶ 195. The SEC's approach would leave companies in limbo about how to comply with both the Exchange Act and Sarbanes-Oxley, knowing only that compliance is virtually impossible and failure virtually guaranteed.

The irony is that the same reasons why the SEC limited the scope of "internal control over financial reporting" under Sarbanes-Oxley counsel equally against expanding "internal accounting controls." As the SEC acknowledged in adopting Rule 13a-15 under Sarbanes-Oxley, accountants

generally have not been responsible for assessing companies' entire internal-control frameworks, nor are they equipped to do so. Adopting Release at 36639-36640. And, of course, the compliance burdens would be massive if companies could be subject to civil or criminal penalties whenever an employee does not comply with an internal policy or the company is a victim of crime.

## III. THE SEC DOES NOT ALLEGE VIOLATIONS OF ACCOUNTING CONTROLS.

The SEC's Complaint does not state facts sufficient to allege that SolarWinds failed "[to] devise and maintain a system of internal *accounting* controls." 15 U.S.C. § 78m(b)(2)(B) (emphasis added). Indeed, the Complaint effectively acknowledges as much. It criticizes SolarWinds's "internal controls" and failure "to devise and maintain a system of internal controls," Compl. ¶¶ 196, 198—which omits the word "accounting" altogether. The SEC believes that "shortcomings" in "SolarWinds' cybersecurity-related policies and procedures" enabled unauthorized access to the company's information systems, source code, and products. Compl. ¶¶ 194-200. But the SEC does not allege that these controls had anything to do with ensuring the reliability of SolarWinds's financial reporting; that the accessed items were assets on the balance sheet; that the hackers' activity caused or could have caused a discrepancy between the company's assets and its accounting for its assets resulting in a material misstatement of the company's financial statements. Compl. ¶ 194-200. In short, as in *SEC* v. *Patel*, the SEC's allegations say "nothing" about "anything . . . that might remotely qualify as an internal accounting control." 2009 WL 3151143, at *26. Facility guards may overlook a policy about who can enter a company's building, but that does not mean the company's financial reporting may be materially false.

Grasping at straws, the SEC says that SolarWinds identified "SOX Control Deficiencies"—*i.e.*, a deficiency in its internal controls over financial reporting under Section 404 of Sarbanes Oxley—with respect to certain password protections. Compl. ¶ 84. But under the SEC's own guidance, a "deficiency" is not a failure of a company's internal control over financial

reporting unless it could have a material effect on the company's financial statements, *see* Interpretive Release at 35332, in which case it must be disclosed, *see* 17 C.F.R. § 240.13a-15(a), (f)(3). Here, SolarWinds and its independent auditor attested to the effectiveness of its internal control over financial reporting in every relevant year, which means that they assessed the deficiency was immaterial. *See, e.g.*, SolarWinds Corp., Annual Report (Form 10-K), at F-2 (Mar. 1, 2021). The Complaint does not allege that this attestation was incorrect or that any deficiency was material, so its stray reference to a "SOX Control Deficiencies" lends no support to its claim.

The SEC also makes the irrelevant allegation that SolarWinds used standards from the COSO Framework to assess its "internal controls." Compl. ¶¶ 196-197. The COSO Framework is explicitly designed for use in assessing *all types* of internal controls. *See* COSO, *Internal Control – Integrated Framework: Executive Summary* 3 (May 2013) (COSO Framework) ("Internal control is a process . . . designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."). Thus, the SEC's allegation only underscores that it sees no distinction between "accounting" and other types of internal controls.[6]

## CONCLUSION

For the foregoing reasons, the Seventh and Eighth Claims for Relief should be dismissed.

---

[6] The SEC selectively quotes from the COSO Framework to suggest incorrectly that it requires all technology controls to be included in a company's internal control over financial reporting. To the contrary, the COSO Framework only provides examples of types of technology controls that may be relevant depending on the company's objective, and even as to those examples, states that it "*does not require*" them. COSO Framework at 97, 24. The SEC further alleges that "under the COSO Framework, SolarWinds chose to use the NIST Framework" to conduct assessments. Compl. ¶ 197. The NIST Framework provides guidance and standards to help mitigate cybersecurity risk. Nat'l Institute of Standards and Tech. (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. *Id.* at 14-15. Companies typically use the NIST Framework to assess what the COSO Framework treats as operational controls, not financial-reporting controls. The SEC does not argue to the contrary.

Respectfully submitted,

s/ *Nicole Friedlander*

Nicole Friedlander
SULLIVAN & CROMWELL LLP
125 Broad Street
New York, New York 10004
Telephone: (212) 558-4000
Facsimile: (212) 558-3588
friedlandern@sullcrom.com

Jeffrey B. Wall (*pro hac vice* pending)
SULLIVAN & CROMWELL LLP
1700 New York Avenue NW, Suite 700
Washington, DC 20006
Telephone: (202) 956-7500
Facsimile: (202) 293-6330
wallj@sullcrom.com

*Counsel for Amici Curiae*

February 2, 2024