

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

SECURITIES AND EXCHANGE	)	
COMMISSION,	)	
	)	
Plaintiff,	)	
	)	Civil Action No. 1:23-cv-09518-PAE
v.	)	
	)	
SOLARWINDS CORP. and TIMOTHY G.	)	ORAL ARGUMENT REQUESTED
BROWN,	)	
	)	
Defendants.	)	
	)	

**MEMORANDUM OF LAW IN SUPPORT OF
DEFENDANTS' MOTION FOR SUMMARY JUDGMENT**

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES.....	ii
PRELIMINARY STATEMENT.....	1
FACTUAL BACKGROUND	3
A. SolarWinds.....	3
B. Mr. Brown.....	3
C. SolarWinds’ Online Security Statement	4
D. The Undisputed Evidence That the Security Statement Was True.....	5
1. NIST Cybersecurity Framework.....	6
2. Role-Based Access Controls.....	8
3. Passwords.....	13
4. Network Monitoring	15
5. Software Development Lifecycle	16
E. The SEC’s Effort to Change Its Theory of Falsity Through Its Expert	18
F. The Lack of Any Significant Evidence of Materiality.....	19
LEGAL STANDARDS.....	20
ARGUMENT.....	22
II. The SEC Cannot Establish Falsity	22
A. There Is No Dispute That SolarWinds Routinely Implemented the Subject Policies—Which Means It Did Not Pervasively Fail to Do So	23
B. The SEC Cannot Avoid Summary Judgment by Making Speculative Inferences from Vague Documents—Especially When Those Inferences Are Contradicted by Witness Testimony and Its Own Concessions	25
C. The SEC Cannot Avoid Summary Judgment by Changing Its Theory of the Case—Especially When the New Theory Makes No Sense.....	33
D. The SEC Cannot Avoid Summary Judgment by Challenging Representations That Are Not Actually in the Security Statement.....	37
III. The SEC Cannot Establish Materiality	39
IV. The SEC Cannot Establish Scienter or Negligence	42
V. The SEC Cannot Establish a Connection with a Securities Transaction	48
CONCLUSION.....	50

TABLE OF AUTHORITIES

CASES

<i>Africa v. Jianpu Tech. Inc.</i> , 2022 WL 4537973 (S.D.N.Y. Sept. 28, 2022).....	38
<i>Alpha Lyracom Space Commc'ns, Inc. v. Comsat Corp.</i> , 968 F. Supp. 876 (S.D.N.Y. 1996), <i>aff'd</i> , 113 F.3d 372 (2d Cir. 1997)	37
<i>Anderson v. Liberty Lobby, Inc.</i> , 477 U.S. 242 (1986).....	21
<i>Anthony v. GE Cap. Retail Bank</i> , 321 F. Supp. 3d 469 (S.D.N.Y. 2017).....	25
<i>Barilli v. Sky Solar Holdings, Ltd.</i> , 389 F. Supp. 3d 232 (S.D.N.Y. 2019).....	22
<i>Boca Raton Firefighters & Police Pension Fund v. Bahash</i> , 506 F. App'x 32 (2d Cir. 2012)	42
<i>Chadbourne & Parke LLP v. Troice</i> , 571 U.S. 377 (2014).....	48, 49
<i>Charles Schwab Corp. v. Bank of Am. Corp.</i> , 883 F.3d 68 (2d Cir. 2018).....	48
<i>City of Coral Springs Police Officers' Ret. Plan v. Farfetch Ltd.</i> , 565 F. Supp. 3d 478 (S.D.N.Y. 2021).....	44
<i>City of Philadelphia v. Fleming Cos.</i> , 264 F.3d 1245 (10th Cir. 2001)	43
<i>Conn. Indem. Co. v. 21st Century Transp. Co.</i> , 186 F. Supp. 2d 264 (E.D.N.Y. 2002)	32
<i>Cordiano v. Metacon Gun Club, Inc.</i> , 575 F.3d 199 (2d Cir. 2009).....	21
<i>D'Addario v. D'Addario</i> , 75 F.4th 86 (2d Cir. 2023)	49
<i>Dalberth v. Xerox Corp.</i> , 766 F.3d 172 (2d Cir. 2014).....	31
<i>DeKalb Cnty. Pension Fund v. Allergan PLC</i> , 2024 WL 677081 (2d Cir. Feb. 20, 2024).....	34, 38

<i>Deng v. 278 Gramercy Park Grp., LLC</i> , 23 F. Supp. 3d 281 (S.D.N.Y. 2014).....	32
<i>Dowd v. IRS</i> , 776 F.2d 1083 (2d Cir. 1985).....	32
<i>ECA & Loc. 134 IBEW Joint Pension Tr. of Chi. v. JP Morgan Chase Co.</i> , 553 F.3d 187 (2d Cir. 2009).....	23, 36, 38, 41
<i>Fernandez v. China Ocean Shipping (Grp.) Co.</i> , 312 F. Supp. 2d 369 (E.D.N.Y. 2003), <i>aff'd</i> , 94 F. App'x 866 (2d Cir. 2004).....	32
<i>Foley v. Transocean Ltd.</i> , 861 F. Supp. 2d 197 (S.D.N.Y. 2012).....	40
<i>FTC v. Moses</i> , 913 F.3d 297 (2d Cir. 2019).....	37
<i>Geffon v. Micrion Corp.</i> , 249 F.3d 29 (1st Cir. 2001).....	47
<i>Gillis v. QRX Pharma Ltd.</i> , 197 F. Supp. 3d 557 (S.D.N.Y. 2016).....	38
<i>Greenhouse v. MCG Cap. Corp.</i> , 392 F.3d 650 (4th Cir. 2004)	41
<i>Gross v. GFI Grp., Inc.</i> , 310 F. Supp. 3d 384 (S.D.N.Y. 2018), <i>aff'd</i> , 784 F. App'x 27 (2d Cir. 2019).....	44
<i>Hemming v. Alfin Fragrances, Inc.</i> , 690 F. Supp. 239 (S.D.N.Y. 1988).....	50
<i>Horror Inc. v. Miller</i> , 15 F.4th 232 (2d Cir. 2021)	21
<i>Howard v. Arconic Inc.</i> , 395 F. Supp. 3d 516 (W.D. Pa. 2019).....	49
<i>In re Allergan PLC Securities Litigation</i> , 2022 WL 17584155 (S.D.N.Y. Dec. 12, 2022), <i>aff'd</i> , 2024 WL 67708 (2d Cir. Feb. 20, 2024)	34
<i>In re Austl. & N.Z. Banking Grp. Ltd. Sec. Litig.</i> , 2009 WL 4823923 (S.D.N.Y. Dec. 14, 2009)	38
<i>In re Citigroup, Inc. Sec. Litig.</i> , 330 F. Supp. 2d 367 (S.D.N.Y. 2004), <i>aff'd</i> , 165 F. App'x 928 (2d Cir. 2006).....	36

<i>In re Constellation Energy Grp., Inc. Sec. Litig.</i> , 738 F. Supp. 2d 614 (D. Md. 2010)	24
<i>In re Heartland Payment Sys., Inc. Sec. Litig.</i> , 2009 WL 4798148 (D.N.J. Dec. 7, 2009)	42
<i>In re Intel Corp.. Sec. Litig.</i> , 2019 WL 1427660 (N.D. Cal. Mar. 29, 2019)	42
<i>In re Marriott Int’l, Inc.</i> , 31 F.4th 898 (4th Cir. 2022)	42
<i>In re Miller Indus., Inc.</i> , 120 F. Supp. 2d 1371 (N.D. Ga. 2000)	39
<i>In re Mylan N.V. Sec. Litig.</i> , 666 F. Supp. 3d 266 (S.D.N.Y. 2023), <i>aff’d</i> , 2024 WL 1613907 (2d Cir. Apr. 15, 2024)	47
<i>In re N. Telecom Ltd. Sec. Litig.</i> , 116 F. Supp. 2d 446 (S.D.N.Y. 2000)	21, 40, 43
<i>In re Oracle Corp. Sec. Litig.</i> , 627 F.3d 376 (9th Cir. 2010)	47
<i>In re Philip Morris Int’l Inc. Sec. Litig.</i> , 89 F.4th 408 (2d Cir. 2023)	22, 25
<i>In re Plains All Am. Pipeline, L.P. Sec. Litig.</i> , 307 F. Supp. 3d 583 (S.D. Tex. 2018)	25
<i>In re Poseidon Concepts Sec. Litig.</i> , 2016 WL 3017395 (S.D.N.Y. May 24, 2016)	46
<i>In re REMEC Inc. Sec. Litig.</i> , 702 F. Supp. 2d 1202 (S.D. Cal. 2010)	33, 45, 48
<i>In re Union Carbide Class Action Sec. Litig.</i> , 648 F. Supp. 1322 (S.D.N.Y. 1986)	24, 36
<i>In re Wachovia Equity Sec. Litig.</i> , 753 F. Supp. 2d 326 (S.D.N.Y. 2011)	46
<i>Inchen Huang v. Higgins</i> , 443 F. Supp. 3d 1031 (N.D. Cal. 2020)	37
<i>Jysk Bed’N Linen v. Dutta-Roy</i> , 787 F. App’x 608 (11th Cir. 2019)	32

<i>Kang v. PayPal Holdings, Inc.</i> , 620 F. Supp. 3d 884 (N.D. Cal. 2022)	24
<i>Karp v. First Conn. Bancorp, Inc.</i> , 535 F. Supp. 3d 458 (D. Md. 2021), <i>aff'd</i> , 69 F.4th 223 (4th Cir. 2023)	47
<i>Kidd v. Midland Credit Mgmt., Inc.</i> , 2019 WL 4736913 (E.D.N.Y. Sept. 27, 2019)	32
<i>Lewy v. SkyPeople Fruit Juice, Inc.</i> , 2012 WL 3957916 (S.D.N.Y. Sept. 10, 2012).....	24, 46
<i>Leykin v. AT & T Corp.</i> , 423 F. Supp. 2d 229 (S.D.N.Y. 2006), <i>aff'd</i> , 216 F. App'x 14 (2d Cir. 2007).....	49
<i>Lindblom v. Mobile Telecomms. Techs. Corp.</i> , 985 F. Supp. 161 (D.D.C. 1997)	50
<i>Lopez v. Gap, Inc.</i> , 883 F. Supp. 2d 400 (S.D.N.Y. 2012).....	34
<i>Matrixx Initiatives, Inc. v. Siracusano</i> , 563 U.S. 27 (2011).....	39, 41
<i>Matsushita Elec. Indus. Co. v. Zenith Radio Corp.</i> , 475 U.S. 574 (1986).....	20
<i>Medis Inv. Grp. v. Medis Techs., Ltd.</i> , 586 F. Supp. 2d 136 (S.D.N.Y. 2008), <i>aff'd</i> , 328 F. App'x. 754 (2d Cir. 2009).....	46
<i>Meiri v. Dacon</i> , 759 F.2d 989 (2d Cir. 1985).....	47
<i>Mirror Worlds Techs., LLC v. Facebook, Inc.</i> , 588 F. Supp. 3d 526 (S.D.N.Y. 2022), <i>aff'd</i> , 122 F.4th 860 (Fed. Cir. 2024).....	31
<i>Mod. Home Inst., Inc. v. Hartford Accident & Indem. Co.</i> , 513 F.2d 102 (2d Cir. 1975).....	33
<i>Noll v. Int'l Bus. Machs. Corp.</i> , 787 F.3d 89 (2d Cir. 2015).....	20
<i>Novak v. Kasaks</i> , 216 F.3d 300 (2d Cir. 2000).....	34
<i>Ong v. Chipotle Mexican Grill, Inc.</i> , 294 F. Supp. 3d 199 (S.D.N.Y. 2018).....	24

<i>Plumber & Steamfitters Loc. 773 Pension Fund v. Danske Bank A/S</i> , 11 F.4th 90 (2d Cir. 2021)	37
<i>Reeves v. Sanderson Plumbing Prods., Inc.</i> , 530 U.S. 133 (2000).....	21
<i>Reidinger v. Zendesk, Inc.</i> , 2021 WL 796261 (N.D. Cal. Mar. 2, 2021), <i>aff'd</i> , 2022 WL 614235 (9th Cir. Mar. 2, 2022).....	24, 46
<i>Savino v. City of New York</i> , 331 F.3d 63 (2d Cir. 2003).....	21
<i>Schlifke v. Seafirst Corp.</i> , 866 F.2d 935 (7th Cir. 1989)	43
<i>Scott v. Harris</i> , 550 U.S. 372 (2007).....	25
<i>SEC v. Enters. Sols., Inc.</i> , 142 F. Supp. 2d 561 (S.D.N.Y. 2001).....	44
<i>SEC v. Ginder</i> , 752 F.3d 569 (2d Cir. 2014).....	45, 47
<i>SEC v. Infinity Grp. Co.</i> , 993 F. Supp. 324 (E.D. Pa. 1998), <i>aff'd</i> , 212 F.3d 180 (3d Cir. 2000).....	48
<i>SEC v. Mahabub</i> , 343 F. Supp. 3d 1022 (D. Colo. 2018), <i>aff'd</i> , 32 F.4th 902 (10th Cir. 2022)	49
<i>SEC v. Monarch Funding Corp.</i> , 192 F.3d 295 (2d Cir. 1999).....	21
<i>SEC v. Morgan</i> , 2019 WL 2385395 (W.D.N.Y. June 5, 2019).....	49
<i>SEC v. Patty</i> , 891 F.2d 295 (9th Cir. 1989)	43
<i>SEC v. Pirate Inv. LLC</i> , 580 F.3d 233 (4th Cir. 2009)	49
<i>SEC v. Riel</i> , 282 F. Supp. 3d 499 (N.D.N.Y. 2017).....	44
<i>SEC v. Shanahan</i> , 646 F.3d 536 (8th Cir. 2011)	45

<i>SEC v. Terry’s Tips, Inc.</i> , 409 F. Supp. 2d 526 (D. Vt. 2006).....	44
<i>SEC v. Yorkville Advisors, LLC</i> , 305 F. Supp. 3d 486 (S.D.N.Y. 2018).....	25, 38, 43, 47
<i>SEC v. Zandford</i> , 535 U.S. 813 (2002).....	48, 49, 50
<i>Self v. Crum</i> , 439 F.3d 1227 (10th Cir. 2006)	32
<i>Shenk v. Karmazin</i> , 868 F. Supp. 2d 299 (S.D.N.Y. 2012).....	39
<i>Sheridan v. Jaffe</i> , 1996 WL 345965 (S.D.N.Y. June 24, 1996)	32
<i>Shields v. Citytrust Bancorp, Inc.</i> , 25 F.3d 1124 (2d Cir. 1994).....	45
<i>Singh v. Cigna Corp.</i> , 918 F.3d 57 (2d Cir. 2019).....	39
<i>Teamsters Loc. 445 Freight Div. Pension Fund v. Dynex Cap. Inc.</i> , 531 F.3d 190 (2d Cir. 2008).....	43
<i>Tieu v. N.Y.C. Econ. Dev. Corp.</i> , 717 F. Supp. 3d 305 (S.D.N.Y. 2024).....	26, 31
<i>TSC Indus., Inc. v. Northway, Inc.</i> , 426 U.S. 438 (1976).....	40
<i>United States v. Naftalin</i> , 441 U.S. 768 (1979).....	48
<i>United States v. Shelton</i> , 784 F. App’x 934 (6th Cir. 2019)	49
<i>USA Certified Merchs., LLC v. Koebel</i> , 262 F. Supp. 2d 319 (S.D.N.Y. 2003).....	32
<i>Vantage Point, Inc. v. Parker Bros.</i> , 529 F. Supp. 1204 (E.D.N.Y. 1981), <i>aff’d</i> , 697 F.2d 301 (2d Cir. 1982).....	32
<i>Weinstock v. Columbia Univ.</i> , 224 F.3d 33 (2d Cir. 2000).....	21

STATUTES

15 U.S.C. § 78bb.....	48
15 U.S.C. § 78j(b)	21, 48
15 U.S.C. § 78q(a)	21, 48

RULES

17 C.F.R. 240.10b-5.....	21, 48
Fed. R. Civ. P. 9(b)	34

OTHER AUTHORITIES

<i>Access Control List</i> , NIST Computer Security Resource Center Glossary	10
<i>Pervasive</i> , Cambridge US English Dictionary.....	35
<i>Systemic</i> , Cambridge US English Dictionary	35

PRELIMINARY STATEMENT

As we have said before, the only party in this case that has made false and misleading statements about SolarWinds' cybersecurity is the SEC. Its Amended Complaint accused SolarWinds of routinely failing to implement policies in its online Security Statement, alleging deficiencies that were "pervasive," "systemic," "widespread," and "long-standing." The SEC relied on these strident allegations to bluff its way past dismissal. But discovery has now shown that SolarWinds did just what the Security Statement said. The SEC all but concedes the point in the Joint Statement of Undisputed Material Facts, where, in a remarkable change of tune, it now admits that SolarWinds routinely implemented each of the challenged policies. That dooms the SEC's fundamental claim that SolarWinds routinely failed to do so.

Though the SEC should have dropped this case long ago, it continues to litigate out of inertia. Having brought the case seeking to expand its regulatory sphere of influence over cybersecurity, that effort failed when the Court properly dismissed its overreaching legal theories. Now, the SEC's case has devolved into a face-saving exercise. But the effort is futile, because discovery has shown that the SEC simply cannot prove falsity, materiality, scienter or negligence, or even the requisite connection to a securities transaction. For each of those independent reasons, the Court should finally put an end to this regulatory misadventure and grant summary judgment.

As to falsity, the SEC now concedes—as it must, in the face of voluminous evidence and uncontradicted testimony—that SolarWinds regularly implemented the policies described in the Security Statement. That point is critical and conclusive, as it negates the SEC's core allegation of pervasive and systemic failures. It does the SEC no good to keep pointing to the documents cited in its Amended Complaint, as none of those documents can support an inference of pervasive failures contrary to what the SEC has conceded. And besides, every testifying witness rejected the SEC's confused interpretations of those documents. Nor can the SEC lower its burden by changing

its theory of the case, as it tries to do by arguing it can prove its claims with just a few incidents of significant “magnitude,” regardless of their “frequency.” Putting aside that the SEC does not point to anything of significant “magnitude,” that is not the theory pled in the Amended Complaint—which alleges *pervasive* failures. The SEC may not switch theories now, and its attempt to do so only confirms that it cannot prove the theory it pled.

The SEC cannot establish materiality either. The only evidence on materiality is testimony from two stock analysts, who both testified they never even saw the Security Statement before this case and do not typically inquire into the cybersecurity controls of companies they follow. The analysts further explained that none of the SEC’s evidence would matter to their analysis without context—which in this case is that SolarWinds routinely did what the Security Statement said. And regardless, the only relevance cybersecurity deficiencies could have to investors is that they imply the risk of cyberattack—which SolarWinds plainly disclosed in its investor filings.

The SEC’s allegations against Tim Brown, too, are shamefully unsupported, as the record does not come close to supporting scienter or negligence. Notwithstanding the SEC’s effort to cast him as the mastermind of a fraudulent scheme to deceive investors via the Security Statement, the undisputed facts show he did not even draft the Security Statement. It was drafted by Mr. Brown’s subordinate, who relied on preexisting, vetted responses to customer inquiries. Mr. Brown merely reviewed the draft, along with several more senior executives and the legal department, and made no significant changes. The notion that he intended or knew the Security Statement would deceive investors is fanciful, as the webpage was published nearly a year before SolarWinds’ IPO, when it did not even *have* any investors. And of course, Mr. Brown had no reason to believe the Security Statement was false because, as the SEC concedes, it fairly reflected SolarWinds’ routine practices—which is all a reasonable investor would expect if they ever read it.

Lastly, in a sign of just how far the SEC has overstepped its mandate, it cannot establish even the requisite connection between the alleged conduct and a securities transaction. The Security Statement was not about securities. It was not sent to investors. It was not intended to induce a securities transaction, and there is no evidence it did. The only purported nexus is that SolarWinds made the statement, and then later sold securities. No court has ever imposed securities fraud liability based on such a tenuous connection, and this Court should not be the first.

FACTUAL BACKGROUND¹

A. SolarWinds

SolarWinds (the “Company”) is a leading developer of network monitoring software. Joint Statement of Undisputed Material Facts (“JS”) ¶ 4. Its products are widely popular and broadly trusted: During the Relevant Period (from October 2018 to January 2021), SolarWinds had over 300,000 customers, including nearly all Fortune 500 companies—as remains true today. JS ¶ 5. SolarWinds conducted its first IPO in 2009 and remained a public company until 2016, when it was acquired in a take-private transaction. JS ¶ 7. SolarWinds conducted a second IPO in October 2018 and remained public until it was again privately acquired in April 2025. JS ¶¶ 7-8. The Company had approximately 3,000 employees during the Relevant Period. JS ¶ 6.

B. Mr. Brown

Mr. Brown joined SolarWinds in July 2017. JS ¶ 11. He has more than thirty years of experience in software development and cybersecurity, as well as eighteen patents in the cybersecurity field. JS ¶¶ 10, 13. Prior to coming to SolarWinds, Mr. Brown was employed at Dell, Inc. as Chief Technology Officer for the company’s portfolio of security products, and was named

¹ Citations to “JS ___” refer to the parties’ Joint Statement of Undisputed Facts (ECF No. 166). Citations to “DS ___” refer to the concurrently filed Defendants’ Statement of Undisputed Material Facts. Citations to “Ex. ___” refer to the exhibits attached to the concurrently filed Declaration of Serrin Turner in Support of Defendants’ Motion for Summary Judgment.

a “Dell Fellow” based on his accomplishments there—a peer-reviewed honor in the field. JS ¶ 12.

During the Relevant Period, Mr. Brown was SolarWinds’ Vice President of Security and Architecture. JS ¶ 15. His duties included, among other things: (1) supervising SolarWinds’ “InfoSec” team, which was responsible for monitoring SolarWinds’ network for security threats and responding to security incidents; and (2) working with SolarWinds’ product teams on building security into product architecture. JS ¶¶ 15-16. Mr. Brown did not hold an executive position. JS ¶ 17. He reported to the Chief Information Officer (CIO), Rani Brown, who in turn reported to Joe Kim, the Chief Technology Officer (CTO), who reported to the CEO. JS ¶ 17.

C. SolarWinds’ Online Security Statement

This case concerns a mundane document added to SolarWinds’ website for mundane reasons. JS ¶¶ 25-30. In 2017, it was becoming increasingly common in the software industry for customers to do some level of cybersecurity diligence on vendors as part of their procurement processes, often via a questionnaire about each vendor’s cybersecurity controls. JS ¶ 27. Such questionnaires could be only a few questions long, or dozens of questions long; it would depend on how important the inquiring company viewed the vendor to be to its business. JS ¶ 38.

Prior to 2017, SolarWinds’ general practice had been to respond to such questionnaires individually over email. JS ¶ 28. Through this practice—which predated Mr. Brown’s arrival at the Company—SolarWinds had developed a database of frequently asked questions, along with answers that relevant subject-matter experts in the Company had vetted and its in-house legal department had approved. JS ¶ 29. In mid-2017, to reduce the growing burden from responding to customer inquiries individually, SolarWinds decided to add a page to its website—the Security Statement—to provide some of the more commonly requested information about its security program, so that customers could find the information on their own. JS ¶ 30.

The Security Statement was published in November 2017. JS ¶ 25. The document was

drafted by Eric Quitugua, who worked as the manager of the InfoSec team under Mr. Brown. JS ¶¶ 31-32. Mr. Quitugua compiled the Security Statement by consolidating content from the Company’s preexisting database of answers to customers’ security questions. JS ¶ 32. To the extent Mr. Quitugua needed any additional information about a topic, he consulted relevant subject-matter experts at the Company. JS ¶ 33. Mr. Quitugua’s draft of the Security Statement was reviewed by Mr. Brown, along with his superiors, Ms. Johnson and Mr. Kim, and an in-house attorney, before it was published. JS ¶ 34. Mr. Brown made no significant changes, and the published version was fairly close to Mr. Quitugua’s draft language. JS ¶ 37.

The Security Statement provided only high-level information about SolarWinds’ security program, of a sort that could be safely disclosed online, and was aimed at customers seeking to do only basic diligence on SolarWinds’ security. JS ¶¶ 39-40. Customers needing more granular information continued to send detailed questionnaires after publication of the Security Statement, which SolarWinds continued to answer separately, after requiring the customers to sign a non-disclosure agreement to protect this more sensitive information. *Id.*

D. The Undisputed Evidence That the Security Statement Was True

The Amended Complaint alleges that SolarWinds had “long-standing, pervasive, systemic, and material cybersecurity deficiencies,” Am. Compl. (“AC”) ¶ 2, as to five specific policies described in the Security Statement, concerning: (1) the NIST Cybersecurity Framework; (2) role-based access controls; (3) password complexity; (4) network monitoring; and (5) secure software development (the “Subject Policies”), AC ¶ 72; *see also* AC ¶¶ 74, 110, 148, 159, 179 (identifying representations at issue). None of these allegations panned out in discovery. The undisputed evidence shows—and both sides agree—that SolarWinds implemented each of the Subject Policies as a routine practice, rendering the SEC’s claims of pervasive deficiencies baseless. *See* JS ¶¶ 64, 70 (NIST); *id.* ¶¶ 74-75, 92-94 (role-based access controls); *id.* ¶¶ 110, 112, 117, 126 (passwords);

id. ¶¶ 129, 132-33, 137 (network monitoring); *id.* ¶¶ 144, 146, 148, 150 (software development).

1. NIST Cybersecurity Framework

Under the heading “Organizational Security,” the Security Statement stated: “SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect, and respond to security incidents.” JS ¶ 41. The SEC alleges this statement was false because it failed to disclose supposed “persistent poor scores” the Company gave itself in self-assessments under the NIST CSF. AC ¶ 91. That allegation is fundamentally confused, and the evidence shows that the statement was true.

The NIST CSF is a voluntary self-assessment framework that an organization can follow to assess its cybersecurity and identify areas of risk or desired improvement. JS ¶¶ 45, 50, 52; *see also* AC ¶ 74 (describing the NIST CSF as “a set of tools that an organization can use as one part of its assessment of its cybersecurity posture”). Importantly, the NIST CSF is not a cybersecurity “standard”—that is, it does not prescribe particular controls that one must adopt in order to “comply.” JS ¶ 47. Rather, the NIST CSF “offers a flexible way to address cybersecurity,” through a process designed to “help an organization to align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources.” JS ¶ 48.

The self-assessment framework is simple. The NIST CSF divides cybersecurity activities into five “Functions”: “Identify, Protect, Detect, Respond, and Recover.” JS ¶ 50. Within each, the NIST CSF lists categories and subcategories of cybersecurity objectives. JS ¶ 52. An organization using the NIST CSF gives itself a numerical score—or “Tier”—for its controls in each category. JS ¶ 53. An organization need not meet any particular score; Tiers do not serve as passing or failing grades. JS ¶ 55. Rather, “Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices.” JS ¶ 54. They “are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the

organization are higher priority and could receive additional resources.” JS ¶ 56.

“To account for the unique cybersecurity needs of organizations, there are a wide variety of ways to use the Framework. The decision about how to apply it is left to the implementing organization.” JS ¶ 60. Organizations are free, for example, to select which NIST CSF categories and subcategories of controls to evaluate, and may even create their own categories to fit their particular needs. JS ¶¶ 57, 61. The essence of following the NIST CSF is for an organization to have a recurring process for evaluating its cybersecurity in order to guide decisions about where to improve and how to allocate resources. JS ¶¶ 51-63. As the NIST CSF states:

[The NIST CSF’s] five high-level Functions ... provide a concise way for senior executives and others to distill the fundamental concepts of cybersecurity risk so that they can assess how identified risks are managed, and how their organization stacks up at a high level against existing cybersecurity standards, guidelines, and practices. The Framework can also help an organization answer fundamental questions, including ‘How are we doing?’ Then they can move in a more informed way to strengthen their cybersecurity practices where and when deemed necessary.

JS ¶ 51.

There is no dispute that SolarWinds followed the NIST CSF as a guide in assessing its cybersecurity program during the Relevant Period. JS ¶¶ 64, 70. In 2017 and 2018, Mr. Quitugua prepared assessments of SolarWinds’ security program explicitly based on “the NIST Cybersecurity [F]ramework.” JS ¶¶ 65-66. They consisted of spreadsheets reflecting security objectives under the five NIST Functions, and numerical scores Mr. Quitugua assigned to them. *Id.* Subsequently, in 2019, Ms. Johnson and Mr. Brown began a practice—which continued through the Relevant Period—of preparing “NIST Scorecards” for quarterly briefings to management. JS ¶¶ 67, 69. These scorecards reflected evaluations of SolarWinds’ “NIST Maturity Level” (*i.e.*, its Tier) in cybersecurity categories under the five NIST Functions. JS ¶ 68. These scorecards helped identify areas where Ms. Johnson and Mr. Brown were seeking to upgrade the Company’s controls, so management could decide how to allocate resources. JS ¶ 69.

Accordingly, the Security Statement’s representation that SolarWinds “follows the NIST Cybersecurity Framework” was true. The Company followed the self-evaluation framework, using it on a recurring basis to identify opportunities for improvement, communicate information to stakeholders, and guide managerial decision-making. JS ¶¶ 65-69. That is precisely how the NIST CSF is meant to be used. JS ¶¶ 55-66. As for the SEC’s allegation that SolarWinds gave itself “persistent poor scores” on these evaluations, AC ¶ 91, the allegation is unfounded: As the Court previously commented, the Company’s NIST Scorecards reflect “a perfectly solid set of evaluations,” MTD Hr’g 43:24-25, ECF No. 120. But more importantly, the allegation is irrelevant. The Security Statement said nothing about what scores SolarWinds gave itself in following the NIST CSF, nor are any particular scores required to follow it. JS ¶¶ 41, 55.

2. Role-Based Access Controls

Under a heading titled, “Access Controls,” the Security Statement stated the following:

Role Based Access

Role based access controls are implemented for access to information systems. Processes and procedures are in place to address employees who are voluntarily or involuntarily terminated. Access controls to sensitive data in our databases, systems, and environments are set on a need-to-know / least privilege necessary basis. Access control lists define the behavior of any user within our information systems, and security policies limit them to authorized behaviors.

Authentication and Authorization

...

SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.

JS ¶ 71. The SEC alleges that SolarWinds’ access controls were “diametrically different from the description in the Security Statement,” asserting that, “[i]n reality, from at least 2017 through at least 2020, ... SolarWinds routinely and pervasively granted employees unnecessary

‘admin’ rights, giving them access and privileges to more systems than necessary for their work functions and violating the concept of ‘least privilege.’” AC ¶¶ 181-82. The undisputed evidence belies this allegation. Witness testimony and abundant documentation show that SolarWinds had role-based access controls in place just as the Security Statement described. JS ¶¶ 74-94.

The concept of “role-based access controls” simply refers to measures designed to provision employees with access rights based on what they need to perform their jobs. JS ¶ 72. The “principle of least privilege” is a related concept that refers to provisioning employees with the minimum access needed to perform their duties. JS ¶ 73. There is no dispute that SolarWinds had measures in place to provision employees with only those access rights needed to perform their roles, consistent with the Security Statement’s representations. JS ¶¶ 74-75, 92.

Specifically, when a new employee was hired at SolarWinds, the employee’s manager would fill out a form—known as a “System Access Request Form” or “SARF”—identifying the employee’s role. JS ¶ 75. Based on that role, the employee would be provisioned with a specifically designated set of access rights—on top of a limited set of access rights that all employees would receive for basic company resources such as email. *Id.* The assignment of these role-based access rights followed a matrix correlating different access rights to different employee roles at the Company. JS ¶¶ 77-86. If the employee needed any access rights beyond those specified for their role in the matrix, those access rights had to be specially requested on the SARF and approved by an appropriate manager or system owner. JS ¶¶ 86-89.

Once a SARF was completed, it would be sent to IT support staff, who would provision the employee with the appropriate access rights. JS ¶ 89. IT support staff did so by generating “tickets” on an internal work-tracking platform to track the steps taken to implement the access rights. *Id.* The tickets included a copy of the SARF, which served as a record of the approval of

the access rights being provisioned. *Id.* At a technical level, IT support staff would grant an employee access to the appropriate systems by adding the employee's user account to the access control lists governing those systems. *Id.*² When an employee was terminated, the same process was followed in reverse: IT support staff would be notified and then work to revoke the access rights the employee had previously been granted, recording their work in internal tickets. JS ¶ 91.

Multiple SolarWinds witnesses testified to these processes being in place during the Relevant Period.³ That testimony is undisputed. It is also comprehensively corroborated by internal policy documentation describing the SARF process, along with thousands of SARF forms and tickets generated during the Relevant Period, reflecting role-based access controls being implemented on a day-to-day basis. JS ¶ 93. Based on this evidence, the SEC's expert repeatedly conceded at his deposition that the SARF process was followed as a routine practice during the Relevant Period.⁴ And the SEC admits the same now. JS ¶ 92.

² An "access control list" refers to a list of users or user groups that determines the level of access each user or group has to a given resource. *See Access Control List*, NIST Computer Security Resource Center Glossary, <https://bit.ly/nistacs> (last visited Apr. 25, 2025).

³ Ex. 59 (Kim Dep.) 79:4-19 ("What [the] SARF [process] was utilized for was ... when somebody would join the company, to be able to give them appropriate access to systems within your organization ..."); Ex. 54 (Quitugua Dep.) 326:8-15, 336:21-337:6 (explaining that a SARF was "basically a request form submitted to kick off the account provisioning process"); Ex. 46 (Brown Dep.) 204:21-205:3 ("We had a manual process to onboard and give appropriate access rights to people called S-A-R-F.").

⁴ Ex. 50 (Graff Dep.) 151:3-21 ("Q. ... [T]he SARF forms were designed to provision users with access based on their role when they arrived at the company. Is that your understanding? A. It was part of the processes of—sure, of provisioning, you bet. ... Q. Right. If I was starting as a, whatever, IT support person, there would be a set of accesses that I would get based on that role, if the SARF process was followed? A. That's right. Q. It sounds like you're not contesting that was done at the company as a routine practice? A. Yeah, I think that's right."); *id.* at 151:22-152:7 ("Q. And then when people left the company, ... [the SARF process] would be followed in reverse, right? ... A. That's the way it was supposed to work, and I know it did work that way in a lot of cases. Q. Right. So with that too, you're not contesting that that was the routine practice of the company? A. No, I'm not contesting that."); *id.* at 58:1-7 ("[A]s I said before, there are several indications from these SARFs, these forms, that there was a practice in place, and they did it correctly many times.").

But the evidence does not end there. SolarWinds also routinely checked the results of the SARF process through quarterly “user access reviews” to ensure it was being implemented correctly. JS ¶¶ 96-98. In these reviews, SolarWinds’ IT team took inventory of user access rights on key systems to confirm that privileges were appropriate and to catch any potential errors in the provisioning or de-provisioning process. *Id.* The SEC does not contest this either. *Id.*

Moreover, SolarWinds’ access-provisioning processes were specifically validated by multiple *external* audits during the Relevant Period. JS ¶ 99. In Sarbanes-Oxley (“SOX”) audits conducted in 2019 and 2020, PricewaterhouseCoopers (“PwC”) repeatedly validated that:

- SolarWinds had an “established and documented” process “for initiating, authorizing, recording, processing, [and] reviewing a request for access rights”;
- “[n]ew users are provisioned access in accordance with the SolarWinds System Groups Matrix”;
- “[a]ny additional access required, including access to super user or admin responsibilities, require approval from manager, IT and/or the system owner”;
- and
- “[w]hen an employee is terminated, access to Active Directory”—the Company’s primary system for managing access rights—“is removed in a timely manner.” JS ¶¶ 100-04.

Separately, multiple outside firms conducted “SOC-2 audits” for several SolarWinds product lines—a type of audit sometimes sought by customers seeking assurance that a vendor has appropriate security controls in place. JS ¶¶ 105-06. These audits, too, specifically validated SolarWinds’ role-based access controls, finding, for example, that “[a]dministrative access” on the audited systems was “limited to appropriate personnel based on job function.” JS ¶¶ 106-07.

As for the SEC’s inflammatory allegation that SolarWinds “routinely and pervasively granted employees unnecessary ‘admin’ rights,” AC ¶ 182, it is pure fiction. Not only did the SARF process operate to ensure that access to sensitive data was granted only to employees who needed it for their role, JS ¶ 94, but, additionally, SolarWinds employed technical safeguards to

prevent employees from improperly receiving such rights. Specifically, SolarWinds’ InfoSec team monitored the Company’s network with a tool known as “Security Event Manager” (itself a SolarWinds product), which was configured to alert the team whenever someone was added to a user group with administrative privileges. JS ¶ 95. Following such an alert, the InfoSec team would check whether the change in access rights was “authorized and intentional,” by conferring with others or by locating a ticket approving the change. *Id.* Again, the SEC does not contest these were SolarWinds’ routine practices, and its own expert admitted that he was unaware of any evidence that SolarWinds “routinely or frequently” granted employees administrative rights.⁵

Accordingly, the undisputed evidence shows the Security Statement’s representations here were true. “Role based access controls” *were* “implemented for access to information systems.” JS ¶¶ 71, 74, 92. “Processes and procedures” *were* “in place to address employees who are voluntarily or involuntarily terminated.” *Id.* Grants of access “to sensitive data”—*e.g.*, network admin rights—were not given out like candy to all employees as the Amended Complaint absurdly imagines; instead, they *were* assigned on a “least privilege necessary basis.” *Id.* The Security Statement itself spells out the key processes the Company followed in this regard:

SolarWinds employees are granted a limited set of default permissions to access company resources, such as their email, and the corporate intranet. Employees are granted access to certain additional resources based on their specific job function. Requests for additional access follow a formal process that involves a request and an approval from a data or system owner, manager, or other executives, as defined by our security guidelines. Approvals are managed by workflow tools that maintain audit records of changes.

Id. This is simply a description of the SARF process—which the SEC does not dispute “was followed as a routine practice by SolarWinds during the Relevant Period.” JS ¶ 92.

⁵ Ex. 50 (Graff Dep.) 160:13-19 (“Did you see evidence that employees pervasively at the company were granted admin rights? A. I saw evidence of some employees being given superuser access rights that weren’t related to their roles, and it happened more than once, but whether that would match the characterization of routinely or frequently, I don’t think so.”).

SolarWinds obviously drafted the language in the Security Statement about access controls to match the processes it actually had—why *wouldn't* it? There is no evidence the Company pervasively granted admin rights to sensitive systems—why *would* it? The SEC's contrary allegations never made any sense and, unsurprisingly, discovery revealed them to be baseless.

3. Passwords

The Security Statement stated the following with respect to passwords:

We require that authorized users be provisioned with unique account IDs. Our password policy covers all applicable information systems, applications, and databases. Our password best practices enforce the use of complex passwords that include both alpha and numeric characters, which are deployed to protect against unauthorized use of passwords.

JS ¶ 109. The Amended Complaint asserts these statements were false and misleading because of supposed “password problems” that allegedly “persisted for years.” AC ¶ 163. The undisputed evidence instead reflects that the statements in the Security Statement were true.

The password representations are limited in what they say. The first sentence simply states that the Company required authorized users on its network to be provisioned with unique account IDs—in other words, unique usernames. JS ¶ 109. The Company did so: authorized users received unique usernames, typically consisting of their first and last names separated by a dot. JS ¶ 111. The second sentence merely represents that SolarWinds had a password policy covering all “applicable” systems, applications, and databases. JS ¶ 109. That was true: SolarWinds had a written password policy that broadly defined the systems, applications, and databases to which it applied. JS ¶ 113. The policy included complexity requirements specifying that passwords should be a certain length and include a combination of alphabetic and nonalphabetic characters. *Id.* SolarWinds' employees were trained on this policy during onboarding. JS ¶ 114.

Finally, the third sentence refers not to the Company's password “policy” but instead to the Company's “best practices,” which were to “enforce” the use of complex passwords. JS ¶ 109.

Enforcing password complexity automatically—so that it is not possible for a user to create a non-complex password—is a “best practice,” in the sense that it is better than only instructing users to follow a password policy. JS ¶ 115. But not all systems allow password complexity to be automatically enforced on user accounts on the system. JS ¶ 116.⁶

SolarWinds routinely enforced password complexity on systems that had such functionality. JS ¶ 117. Most significantly, SolarWinds did so on Active Directory—a Microsoft service that SolarWinds used to manage access to the Company’s internal network. JS ¶ 118-121. Again, multiple witnesses testified to this,⁷ corroborated by contemporaneous documentation, JS ¶¶ 118-19. Active Directory controlled access to most systems used by SolarWinds employees, so enabling the password complexity setting on Active Directory automatically ensured that most systems used by employees were only accessible via a complex password. JS ¶ 121.

Moreover, as with the SARF process, SolarWinds’ password controls were repeatedly audited and found to be in place. JS ¶¶ 122-24. As part of the SOX audits conducted during the Relevant Period, PwC evaluated whether SolarWinds “maintain[ed] password requirements for all financially significant systems and databases, including ... password complexity, as allowed by the application, system, or database.” JS ¶ 122. PwC specifically looked at Active Directory (among other systems) in evaluating this control, and found no material weakness or significant

⁶ For example, a law firm might be able to configure its own network to automatically enforce complex passwords for user accounts on the network. But its lawyers may also need to access an external application, like LEXIS or Westlaw, using separate credentials. The law firm may not be able to automatically enforce its own password requirements on such applications because it does not control those applications, and the applications may not provide a feature that allows a corporate customer to set password requirements for its employees who use the applications.

⁷ See Ex. 54 (Quitugua Dep.) 334:1-21 (“It was enforced through active directory group policy. ... That basically—that technical policy basically states that if you were to type in a password that didn’t meet its complexity and length requirements, that you would not be allowed to create that password.”); Ex. 46 (Brown Dep.) 117:5-15 (“[Active Directory] forced password changes. That has the password complexity enforced.”).

deficiency. JS ¶¶ 123-24; *see also* Campbell Decl. (explaining these terms). Separately, in SOC-2 audits, other outside accounting firms assessed password controls for in-scope systems and found complexity requirements in place. JS ¶ 125.

The above evidence shows that SolarWinds’ password policy included complexity requirements, and that, wherever possible, SolarWinds enforced those requirements automatically as a general practice. In the face of this, the SEC’s expert conceded at his deposition that he did not have any evidence that the use of non-complex passwords “was a frequent problem” at SolarWinds.⁸ Likewise, the SEC concedes that SolarWinds “routinely enforced password complexity on systems that had such functionality.” JS ¶ 117.

4. Network Monitoring

The SEC alleges that representations under the headings “Change Management,” “Auditing and Logging,” and “Network Security,” *see* JS ¶ 127, were false because SolarWinds supposedly had “widespread and persistent failures regarding network monitoring” stemming from a “systemic, organizational-level failure to employ adequate policies and procedures.” AC ¶¶ 157-58. Discovery proved these allegations, too, to be unfounded—so much so that the SEC recently told Defendants it does not intend to pursue them further. But they remain in the Amended Complaint, so Defendants briefly address them here.

First, it was true that SolarWinds monitored configuration changes as they were rolled out on its network, as stated under “Change Management.” JS ¶¶ 128-29. It was also true, as represented under “Auditing and Logging,” that “[n]etwork components, workstations, applications and ... monitoring tools” were “enabled to monitor user activity.” JS ¶¶ 127. This

⁸ Ex. 50 (Graff Dep.) 259:4-9 (“Q. So you have no evidence that it was a frequent occurrence at SolarWinds to use noncomplex passwords? A. Frequent? I didn’t really address frequency. ... I don’t think I have evidence that shows it was a frequent problem.”).

should come as no surprise, as SolarWinds *makes network monitoring software* designed for this very purpose—including the “Security Event Manager” application mentioned above, which SolarWinds used to monitor its own network. JS ¶¶ 132-33. And it is true, as represented under “Network Security,” that SolarWinds used next-generation firewalls to monitor traffic to, from, and within its network. JS ¶ 137.

Accordingly, there is no evidence of any “widespread and persistent failures” to conduct network monitoring, as the SEC’s expert acknowledged at his deposition.⁹ The very idea that SolarWinds—a maker of network monitoring software—would fail to monitor its own network is preposterous. As SolarWinds’ Senior Director of IT testified: “[W]e created network monitoring software. That’s what we did as a business. ... So our maturity of our monitoring was extreme.” Ex. 49 (Cline Dep.) 220:10-12, 220:22-221:2. That the SEC fired off incendiary allegations otherwise in its Amended Complaint, only now to sheepishly abandon them, speaks volumes about the shoddiness of its pre-suit investigation and the recklessness with which it has pursued this case.

5. Software Development Lifecycle

The Security Statement represented the following about SolarWinds’ software development practices:

Software Development Lifecycle

We follow a defined methodology for developing secure software that is designed to increase the resiliency and trustworthiness of our products. Our products are deployed on an iterative, rapid release development lifecycle. Security and security testing are implemented throughout the entire software development methodology. Quality Assurance is involved at each phase of the lifecycle and security best practices are a mandated aspect of all development activities.

Our secure development lifecycle follows standard security practices including vulnerability testing, regression testing, penetration testing, and product security

⁹ Ex. 50 (Graff Dep.) 150:2-13 (“Q. [I]f [SolarWinds] had documented numerous issues with network monitoring over the years [as alleged in the SEC’s complaint], wouldn’t there be evidence that they were aware of deficiencies ... [?] A. Quite likely. Q. Okay. Did you see any evidence like that, yes or no? ... A. Not that I recall.”).

assessments. The SolarWinds architecture teams review our development methodology regularly to incorporate evolving security awareness, industry practices and to measure its effectiveness.

JS ¶ 140. The Amended Complaint alleges this was false and misleading based on a supposed “continuous, systemic failure—lasting from at least January 2018 to at least July 2020—to implement the [secure development lifecycle] that SolarWinds claimed to follow,” AC ¶ 134, including “routinely fail[ing]” to conduct security testing, AC ¶¶ 120, 235. Once again, the undisputed record shows these allegations to be unfounded.

The specific representations SolarWinds made about its “secure development lifecycle” were that the Company conducted “vulnerability testing, regression testing, penetration testing, and product security assessments.” JS ¶ 140. The term “vulnerability testing” means testing code for potential vulnerabilities, often through automated scanning tools. JS ¶ 141. The term “regression testing” refers to testing changes in software to verify that it works as expected. JS ¶ 142. The term “penetration testing” describes testing that simulates techniques a hacker might use to compromise software. JS ¶ 143. The term “product security assessment” is not a term of art and simply refers to assessing the security of a product. JS ¶¶ 150-52.

SolarWinds did all these things as a regular part of its software development lifecycle throughout the Relevant Period. JS ¶¶ 144, 146, 148, 150. Multiple witnesses testified to this.¹⁰ And extensive documentation corroborates their testimony: There are, for example, numerous reports generated from vulnerability scans run during the development process; numerous records of regression tests run on code changes; numerous reports from penetration tests conducted on

¹⁰ Ex. 60 (Colquitt Dep.) 48:1-23 (“We were doing testing, we were doing ... penetration testing”), 119:13-120:20 (testifying his teams did penetration testing); Ex. 59 (Kim Dep.) 116:14-118:11 (“[A]s stated here, things like ... penetration testing ... were conducted on the products as part of the SDLC.”), 134:14-135:10 (same); Ex. 46 (Brown Dep.) 132:17-135:7 (testifying “Software Development Life Cycle” part of the Security Statement “was accurate”).

various products; and numerous “Final Security Reviews” that development teams prepared before launching software releases. JS ¶¶ 145, 147, 149, 153-55; Ex. 2 (Rattray Rep.) ¶ 96.

Yet again, in light of this evidence, the SEC’s expert conceded at his deposition that SolarWinds did security testing of software as a routine practice during the Relevant Period,¹¹ and the SEC makes the same concession now. JS ¶¶ 142-148. Discovery did not yield evidence of any “systemic” or “routine” failures in this regard as the SEC alleged.

E. The SEC’s Effort to Change Its Theory of Falsity Through Its Expert

The SEC’s response to the evidence after fact discovery was to attempt to change its theory of the case, through the report submitted by its putative expert, Mark Graff. The flaws in Mr. Graff’s opinions are addressed in detail in Defendants’ motion to exclude his testimony filed contemporaneously herewith. But most noteworthy for purposes of this motion is that Mr. Graff—who had the opportunity to survey all the evidence produced to the SEC—expressly disclaimed any finding that SolarWinds deviated from the Subject Policies with any “frequency.” Ex. 4 (Graff Rebuttal Report (“GRR”)) ¶ 7. As noted above, he repeatedly acknowledged at his deposition that SolarWinds followed the Subject Policies as a routine practice.

Mr. Graff thus focuses on just a few incidents (recycled throughout his report) that he

¹¹ Ex. 50 (Graff Dep.) 269:6-11 (“Am I right that you’re not contesting that SolarWinds carried out vulnerability testing as part of its software development life cycle? A. Yes, I think they did vulnerability testing in many cases, probably most cases, in terms of product development.”), 281:10-19 (“Q. Mr. Rattray [SolarWinds’ expert] cited 2,000 JIRA tickets reflecting regression testing being conducted. Did you look at those at all? A. I did review a few. Q. Would you consider that to be evidence that regression testing was done as a regular practice as part of the secure development lifecycle? A. I think it’s—yes, I think that is evidence that they conducted regression testing with some regularity.”), 280:2-24 (“Q. ... The bottom line, Mr. Graff, you’re not contesting that pen testing was done most of the time. You’re basically contending that you think they could have done a better job qualitatively with it, fair? A. I’m going to just double check, but I think that’s right. ... [M]ost of the time I think they did do penetration testing as it relates to products.”), 285:5-10 (“Q. So did you look at the JIRA tickets that were cross-referenced in the [Final Security Reviews]? A. I looked at several of them. Q. And did they reflect testing or analysis of code and assessments of risks? A. Yes, many of them did.”).

claims were “inconsistent with” the Security Statement, and asserts that the “magnitude” of these incidents is somehow “indicative” of “systemic” problems. *See, e.g.*, Ex. 3 (Graff Report (“GR”)) ¶¶ 12, 25, 29, 38-39. Mr. Graff makes no effort to identify any standard he used to evaluate the supposed “magnitude” of these incidents, or how it could indicate anything about how “systemic” the underlying conduct was—especially when “systemic” basically means “frequent,” a topic on which Mr. Graff claims to have no opinion. Ex. 4 (GRR) ¶ 15 (asserting he “never stated anything about the frequency of an issue.”).¹²

In essence, after the SEC’s original theory of the case—that there were “pervasive” and “widespread” failures to implement the Subject Policies—did not pan out, Mr. Graff sought to introduce a different theory, focused not on the “frequency” of any supposed failures but rather on the “magnitude” of a few. The SEC has not, of course, sought to amend its complaint to reflect this new theory, which would be futile as the amendment deadline set by the Court has long passed.

F. The Lack of Any Significant Evidence of Materiality

Finally, just as discovery failed to yield evidence of falsity, it also failed to yield evidence of materiality. With no securities expert, event study, relevant stock price movement, or investors who claim to have been misled, the SEC is left to rely solely on the testimony of two stock analysts who followed SolarWinds. But neither analyst testified—or was in a position to testify—that any purported misrepresentations in the Security Statement would be material to the advice they offered to investors.

¹² In contrast, Defendants’ expert, Dr. Greg Rattray—who, unlike Mr. Graff, has extensive experience conducting cybersecurity assessments for large organizations—conducted a straightforward exercise in which he examined the contemporaneous documentation generated from the implementation of the Subject Policies during the Relevant Period, in a similar manner as he would typically do in conducting a cybersecurity assessment in the field. Ex. 2 (Rattray Rep.) ¶ 2. Dr. Rattray concluded that the evidence readily showed that the Subject Policies were regularly implemented in practice by SolarWinds, *id.* ¶ 3—which, again, the SEC is not even contesting at this point.

To the contrary, both analysts testified that, even though they worked to collect any information relevant to investors, they never even *looked at* the Security Statement before the SEC showed it to them in this litigation.¹³ Nor did they ever ask about SolarWinds’ cybersecurity practices during investor calls with the Company or one-on-one discussions they had with management.¹⁴ No buyer ever asked them about SolarWinds’ cybersecurity practices either.¹⁵ The SEC showed the analysts various documents from the Amended Complaint and tried to elicit testimony that the analysts would have considered them material. But both made clear that analysts typically do not see companies’ internal documents, and that, if they had been shown these, they would have lacked sufficient context to understand whether they were about anything material.¹⁶

LEGAL STANDARDS

“Summary judgment must be granted if ‘there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.’” *Noll v. Int’l Bus. Machs. Corp.*, 787 F.3d 89, 93-94 (2d Cir. 2015). For a dispute to be genuine, the nonmovant “must do more than simply show that there is some metaphysical doubt as to the material facts.” *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986). Rather, the evidence must be “such that a reasonable jury could return a verdict for the nonmoving party” under the applicable standard

¹³ Ex. 51 (Hedberg. Dep.) 67:16-23; Ex. 58 (Thill Dep.) 133:17-23.

¹⁴ Ex. 51 (Hedberg. Dep.) 170:10-171:5; Ex. 58 (Thill Dep.) 134:10-135:22.

¹⁵ Ex. 58 (Thill Dep.) 137:6-16 (“So I can say, after 25 years, I’ve never been asked by a buyer, how would you grade their cyber hygiene.”).

¹⁶ Ex. 58 (Thill Dep.) 144:2-22 (“Q. So if—if one of the documents that you were shown here today somehow was magically dropped in your lap, you would want to make sure you had all the relevant context before you relied on it in advising your investors, right? A. Yes. ... Q. And you don't know, do you, whether you have all the context that you need to accurately understand the internal documents that have been shown to you here today? A. I don't.”); Ex. 51 (Hedberg Dep.) 203:12-17 (“Q. And that’s one of the reasons, perhaps, that companies don’t disclose everything going on in their company, because one particular document taken out of context may be misconstrued; correct? A. Correct.”).

of proof. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986).

Importantly, although “reasonable” factual inferences are to be drawn in the nonmovant’s favor, “the court should give credence to ... ‘evidence supporting the moving party that is uncontradicted and unimpeached.’” *Reeves v. Sanderson Plumbing Prods., Inc.*, 530 U.S. 133, 151 (2000). “When a motion for summary judgment is supported by documentary and testimonial evidence, the nonmoving party may not rest upon mere allegations or denials.” *Horror Inc. v. Miller*, 15 F.4th 232, 240 (2d Cir. 2021). Instead, “[t]he time has come ... ‘to put up or shut up.’” *Weinstock v. Columbia Univ.*, 224 F.3d 33, 41 (2d Cir. 2000). “Summary judgment is appropriate, therefore, if the evidence presented by the nonmoving party ‘is merely colorable, or is not significantly probative,’ or if it is based purely on ‘conjecture or surmise.’” *Savino v. City of New York*, 331 F.3d 63, 71 (2d Cir. 2003) (citations omitted).

A claim for securities fraud under Exchange Act § 10(b) and Rule 10b-5 requires the SEC to establish by a preponderance of the evidence that Defendants “(1) made a material misrepresentation ...; (2) with scienter; (3) in connection with the purchase or sale of securities.” *SEC v. Monarch Funding Corp.*, 192 F.3d 295, 308 (2d Cir. 1999). Securities Act § 17(a) requires largely the same elements, except negligence suffices for (a)(2) and (a)(3). *Id.* Because the SEC bears “the burden of proof at trial,” it is sufficient for Defendants “to point to a lack of evidence” on a single “essential element of the [SEC]’s claim.” *Cordiano v. Metacon Gun Club, Inc.*, 575 F.3d 199, 204 (2d Cir. 2009). “A failure of proof on any one of these” elements “‘necessarily renders all other facts immaterial’ and requires summary judgment in favor of defendants.” *In re N. Telecom Ltd. Sec. Litig.*, 116 F. Supp. 2d 446, 455 (S.D.N.Y. 2000).

ARGUMENT

II. The SEC Cannot Establish Falsity

If a “statement was not false,” it “may not form the basis of a Securities Act claim.” *Barilli v. Sky Solar Holdings, Ltd.*, 389 F. Supp. 3d 232, 256 (S.D.N.Y. 2019); *see In re Philip Morris Int’l Inc. Sec. Litig.*, 89 F.4th 408, 430 (2d Cir. 2023) (explaining it is “axiomatic” that “true statements” are not actionable). The SEC cannot show the Subject Policies were false, because there is no genuine dispute SolarWinds implemented them as a regular practice. Therefore, the SEC cannot show the “pervasive” failures alleged as the basis for falsity in the Amended Complaint. No pervasive failures, no falsity. End of story.

All the SEC does is try to distract from its lack of evidence, through three recurring tactics (reflected in its pre-motion letter and expert report). First, the SEC rehashes the same vague notations from the same handful of documents cited in the Amended Complaint, seemingly believing that if it can string enough cherry-picked quotations together it can survive summary judgment in the same fashion it survived dismissal. But discovery has now been completed, in which witnesses uniformly testified that the cited documents were not about any pervasive failures to implement the Subject Policies; nor can the SEC argue otherwise given its concession that the Subject Policies were routinely implemented. Second, the SEC abandons its “pervasiveness” theory, arguing there need only be a few instances when SolarWinds supposedly deviated from the Subject Policies for the evidence to “indicate” “systemic problems.” But that is not the falsity theory pled in the Amended Complaint, nor does it make sense: Issues that are not frequent or widespread are by definition not “systemic.” Third, unable to disprove what the Security Statement actually says, the SEC reads policies into the Security Statement it does not contain and argues falsity with respect to those. But unmentioned policies are irrelevant, and if any language in the

Security Statement were vague enough to encompass them it would amount to puffery.

A. There Is No Dispute That SolarWinds Routinely Implemented the Subject Policies—Which Means It Did Not Pervasively Fail to Do So

The evidence is undisputed that SolarWinds implemented the Subject Policies as a routine practice: Witnesses testified to that; ample documentation corroborates it; and the SEC’s expert admits it. Most importantly, the SEC does not contest it in the Joint Statement of Undisputed Material Facts.¹⁷ That dooms the SEC’s case—because it means SolarWinds did *not* pervasively *fail* to implement the Subject Policies as the Amended Complaint alleges.

Recall the SEC’s strident accusations. The Amended Complaint alleges falsity based on supposedly “long-standing, pervasive, systemic, and material cybersecurity deficiencies” as to the Subject Policies. AC ¶ 2. Such allegations appear throughout the Amended Complaint. It alleges, for example, that SolarWinds “routinely and pervasively granted employees unnecessary ‘admin’ rights,” *id.* ¶ 182, that the Company “Pervasively Failed To Develop Software in a Secure Development Lifecycle,” *id.* ¶¶ 114-15, that there were “password problems” that “persisted for years,” *id.* ¶ 163, and that there were “widespread and persistent failures regarding network monitoring,” *id.* ¶ 157. “These were not isolated instances of an employee failing to adhere to a policy,” the Amended Complaint intoned, “but systemic, organizational-level failures to employ adequate policies and procedures.” *Id.* ¶¶ 102, 158; *see id.* ¶¶ 2, 134, 154, 177, 200, 233 (similar).

It is no accident that the Amended Complaint alleges “pervasive” and “systemic” deficiencies. Such deficiencies are required as a matter of law to prove the falsity of a company’s statement about a policy it has in place, because no reasonable investor would construe a policy statement as “a guarantee” that the company would “prevent failures in its ... practices.” *ECA &*

¹⁷ JS ¶¶ 64, 70 (NIST); *id.* ¶¶ 74-75, 92-94 (role-based access controls); *id.* ¶¶ 110, 112, 117, 126 (passwords); *id.* ¶¶ 129, 132-33, 137 (network monitoring); *id.* ¶¶ 144, 146, 148, 150 (secure software development).

Loc. 134 IBEW Joint Pension Tr. of Chi. v. JP Morgan Chase Co., 553 F.3d 187, 206 (2d Cir. 2009); *see Kang v. PayPal Holdings, Inc.*, 620 F. Supp. 3d 884, 899 n.2 (N.D. Cal. 2022) (holding that “violations would need to be frequent or widespread” to establish falsity, because “statements of compliance here did not ‘reasonably suggest that there would be no violations’”); *In re Constellation Energy Grp., Inc. Sec. Litig.*, 738 F. Supp. 2d 614, 631 (D. Md. 2010) (“A reasonable investor could not assume” from statements about internal controls “that the company would never lapse in these tasks.”). That principle is particularly apposite here, because cybersecurity is technically complex and involves continuous efforts to identify and remediate deficiencies. As the SEC’s expert himself puts it: “[N]o organization has perfect security and ... any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed.” Ex. 3 (GR) ¶ 25; *see Reidinger v. Zendesk, Inc.*, 2021 WL 796261, at *7-8 (N.D. Cal. Mar. 2, 2021) (dismissing claim because defendant “never stated that its employees had unfailingly complied with [third-party] best practices [or] its own best practices” with respect to cybersecurity), *aff’d*, 2022 WL 614235 (9th Cir. Mar. 2, 2022).

Accordingly, to prove the Subject Policies false, it is not enough for the SEC to “merely quibble with [SolarWinds’] execution of those programs and procedures.” *Ong v. Chipotle Mexican Grill, Inc.*, 294 F. Supp. 3d 199, 232 (S.D.N.Y. 2018). The SEC must instead show deficiencies so “long-standing, pervasive, systemic, and material,” AC ¶ 2, as to imply the policies were essentially “never followed” at all. *See Lewy v. SkyPeople Fruit Juice, Inc.*, 2012 WL 3957916, at *20 (S.D.N.Y. Sept. 10, 2012) (requiring “repeated or constant” failures indicating “the policy was never followed during the [relevant] period,” which cannot be shown where defendant “adhered to, or at least endeavored to adhere to, the announced policy”); *In re Union Carbide Class Action Sec. Litig.*, 648 F. Supp. 1322, 1328 (S.D.N.Y. 1986) (statements about

safety controls not misleading where company “knew that there were safety defects, but that steps were being taken to remedy these difficulties”); *In re Plains All Am. Pipeline, L.P. Sec. Litig.*, 307 F. Supp. 3d 583, 620-21 (S.D. Tex. 2018) (failures to implement programs in some areas “do not undermine the general proposition that [the defendant] ... had and implemented programs”).

Despite years of pre-suit investigation, and discovery lasting over a year, the SEC lacks any evidence that SolarWinds pervasively failed to implement the Subject Policies. It concedes that SolarWinds implemented the Subject Policies on a “routine” basis.¹⁸ That necessarily means that there were *not* any failures to implement the practices at issue that were “pervasive,” “systemic,” “routine,” “widespread,” and so on; if a practice is implemented routinely, there is no routine *failure* to implement it. Accordingly, the SEC’s allegations are “blatantly contradicted by the record,” and the Court “should not adopt that version of the facts for purposes of ruling on a motion for summary judgment.” *Scott v. Harris*, 550 U.S. 372, 380 (2007); see *In re Philip Morris*, 89 F.4th at 430; *SEC v. Yorkville Advisors, LLC*, 305 F. Supp. 3d 486, 519 (S.D.N.Y. 2018) (granting summary judgment where “the record [was] replete with instances in which” defendant employed practice it allegedly failed to employ); *Anthony v. GE Cap. Retail Bank*, 321 F. Supp. 3d 469, 474 (S.D.N.Y. 2017) (“allegations are not enough to raise a genuine dispute of material fact when documentary evidence clearly indicates the opposite”).

B. The SEC Cannot Avoid Summary Judgment by Making Speculative Inferences from Vague Documents—Especially When Those Inferences Are Contradicted by Witness Testimony and Its Own Concessions

Rather than disputing the evidence that SolarWinds implemented the Subject Policies, the SEC tries to ignore it, by clinging to the same hodgepodge of documents it quoted in the Amended

¹⁸ JS ¶¶ 64, 70 (NIST); *id.* ¶¶ 74-75, 92-94 (role-based access controls); *id.* ¶¶ 110, 112, 117, 126 (passwords); *id.* ¶¶ 129, 132-33, 137 (network monitoring); *id.* ¶¶ 144, 146, 148, 150 (secure software development).

Complaint. Unlike at the pleading stage, however, the SEC’s allegations about these documents—that they concerned pervasive failures to follow the Subject Policies—no longer are entitled to the Court’s deference. The SEC had years of investigation and discovery to develop *evidence* that the documents had this meaning—and it came up empty. Witnesses emphatically rejected the SEC’s reading of these documents. And in any event, it makes no sense for the SEC to continue insisting that the documents concern pervasive failures to follow the Subject Policies, given the SEC’s own concessions that the Subject Policies were routinely implemented.

The SEC cannot get to trial by simply plugging its ears to witnesses’ uncontradicted testimony and asserting that their favored documents speak for themselves. Courts regularly grant summary judgment where knowledgeable witnesses deny the nonmovant’s interpretation of out-of-court statements. Just last year, in *Tieu v. New York City Economic Development Corp.*, the plaintiff, like the SEC here, interpreted communications between the defendant’s employees as proving an element of her claim. 717 F. Supp. 3d 305, 330 (S.D.N.Y. 2024). But unimpeached testimony by the author of those communications rejecting the plaintiff’s interpretation settled the matter, requiring summary judgment to be granted to the defendant. As Judge Torres explained, “[a]lthough the Court is required to draw reasonable inferences in favor of the plaintiff, a conflict between sworn testimony and conjecture is insufficient to create a genuine issue of fact.” *Id.* The SEC recreates that very scenario with document after document.

Defendants should not have to play document whack-a-mole with the SEC, rebutting each speculative inference the SEC makes from them, when there is no dispute between the parties that SolarWinds regularly implemented the Subject Policies, and the SEC thus cannot read the documents to imply otherwise without contradicting itself. Moreover, page limits prevent Defendants from attempting in this brief to dispel the SEC’s misguided interpretation of every

document it seeks to rely on. However, the following examples are illustrative. Defendants respectfully refer the Court to Defendants’ Statement of Undisputed Material Facts for a fuller accounting of the SEC’s cited documents.

January 2018 Project Update Slide. A typical example is a note the SEC plucks from an early-2018 slide deck with status updates on various projects, in which one slide states, under the heading “Issues, Risks, & Dependencies,” “Concept of least privilege not followed as a best practice.” JS ¶ 178. The note is meaningless without more context; indeed, the SEC’s own expert admitted that he “can’t tell exactly what [the author] might have been referring to” or “what incident or issue led to that notation.” Ex. 50 (Graff Dep.) 195:11-25. There is no need to speculate, though, as the author himself—Mr. Quitugua—testified that the note “doesn’t indicate ... a problem across the organization.” DS ¶ 90. Rather, the slide was about an audit being done to *check* for any instances where privileges were not properly configured—as reflected in the project components listed on the other side of the slide (*e.g.*, “Conduct risk audit and risk assessment against privileged and non-privileged user accounts”). DS ¶ 89. There was no finding of any systemic failure, and the note was not meant to convey that.

NIST Scorecard. Another example is a NIST Scorecard from August 2019 that lists a “1” as the score for “Authentication, Authorization and Identity Management” and contains a bullet (among others) stating: “Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures.” JS ¶ 177. As multiple witnesses testified, these notations did not concern any systemic failure to implement role-based access controls. DS ¶ 30. Rather, they concerned an ongoing project to make the Company’s access-provisioning processes more *automated* and thereby reduce the potential for error. DS ¶ 31. As explained above, SolarWinds had the SARF process in place throughout the Relevant Period, which provisioned employees with

access based on their role, JS ¶ 92; but implementing those access rights at a technical level required IT personnel to manually configure the access control lists of any systems to which an employee needed access, JS ¶¶ 89-91. The more systems that needed to be separately configured, the more chances there were for errors, of the sort SolarWinds would sometimes catch in user access reviews. DS ¶¶ 22-23. This was particularly an issue given the growth of cloud-based software services during this time, which SolarWinds was increasingly using, and which could not be configured with the standard version of Active Directory. DS ¶¶ 23-24.

For this reason, SolarWinds was migrating to Microsoft “Azure” Active Directory (“Azure AD”)—an access management system that could integrate with third-party services, avoiding the need to separately provision users on those services. DS ¶¶ 24, 28, 31. As SolarWinds’ CIO testified, SolarWinds was seeking “a single pane of glass” that would provide a “centralized and standardized ... single authoritative source of identity for the entire company versus having separate identity stores.” Ex. 52 (Johnson Dep.) 102:25-104:1, 185:18-186:3. Multiple witnesses testified this is what the comments in the NIST Scorecard were about—and the audience for the presentation would have understood that from the in-person discussion. DS ¶¶ 30, 36. Indeed, another note on the slide reflects that the Azure AD project was what the Company was doing to “improve” its “processes and procedures” for provisioning access: “Movement to make Azure AD authoritative source of identity. Plan to enable federation for all critical assets.” DS ¶ 32.¹⁹

None of this contradicts anything in the Security Statement, which said nothing about whether the Company used a centralized tool like Azure AD to automate access provisioning. It merely stated at a general level that SolarWinds had processes to assign access based on users’

¹⁹ A draft of the slide specifically notes, next to the “1” score, that the “KPI” (key performance indicator) driving this score was the “[n]umber of assets (mission/business critical) with AD Authentication enabled vs. not enabled”—*i.e.*, the number of assets that had been integrated with Azure AD to date. DS ¶ 33.

roles. SolarWinds *did* have such processes in place—the SARF process. JS ¶¶ 74-75, 92. It was a relatively manual process, but the Security Statement did not represent otherwise.²⁰ That SolarWinds was looking to *improve* its processes by making them more automated does not imply that it failed to implement the basic processes the Security Statement described.

FedRAMP “Preliminary Review.” A last example is a “preliminary review” prepared by Kellie Pierce—an employee working under Rani Johnson, the CIO—concerning FedRAMP certification, JS ¶ 174, which is necessary to sell cloud software to the federal government, DS ¶ 46. The SEC cites this document throughout the Amended Complaint as if it were evidence of pervasive failures to implement the Subject Practices. *See, e.g.*, AC ¶¶ 97-102. The uncontradicted record shows it is nothing of the sort.

As Ms. Johnson, Ms. Pierce, and others testified, the document was prepared in response to a request from SolarWinds’ cloud business line—a small portion of the Company’s overall business—to estimate how much cost and effort it would take to obtain FedRAMP certification. DS ¶ 48. SolarWinds’ cloud business team wanted to sell products to the federal government, but Ms. Johnson believed obtaining FedRAMP certification would be very expensive because the standards were notoriously difficult to meet. DS ¶ 59. In this context, Ms. Johnson asked Ms. Pierce to do a “very cursory, very preliminary” assessment of the cost and effort required, as she expected that the government sales would not be worth the investment. DS ¶ 60. In other words, this was a *budgeting exercise—not a security assessment*.

Ms. Pierce prepared a spreadsheet, which she specifically labeled a “*preliminary review*,” of the 325 FedRAMP controls along with comments as to whether she believed a documented

²⁰ The SEC’s expert acknowledged this at his deposition. *See* Ex. 50 (Graff Dep.) 242:21-24 (acknowledging that the Security Statement “doesn’t specifically talk about automation” and that using automation is “not the only way to do a good job on account management”).

“program” was in place to demonstrate each control. DS ¶¶ 44-45. As Ms. Pierce testified, the document was never meant to be an authoritative assessment of whether these controls were in place. DS ¶¶ 48, 50, 56-57. Ms. Pierce explained she was “not a technical person,” “not a FedRAMP expert,” and did not “have a good technical understanding of what [the] language in the [FedRAMP] technical controls actually meant.” DS ¶ 63. She played a coordination role at SolarWinds and had no substantive responsibility for SolarWinds’ security practices. DS ¶ 61. Her comments in the spreadsheet were merely her “best guess” from reading the language of each control and seeing if she recalled similar language in SolarWinds’ policies she had reviewed in the past in coordinating SOC-2 audits. DS ¶ 64-65. It was, as Ms. Pierce characterized it, a “quick and dirty” exercise. DS ¶ 48. As another witness familiar with the project put it, Ms. Pierce was “more or less spitballing” to come up with a rough budget estimate for the cloud business team. *Id.*

Besides, Ms. Pierce’s “preliminary review” was not even *about* the Subject Policies. It was about FedRAMP controls—which go far beyond the basic policies in the Security Statement. DS ¶¶ 47, 50-55. And most FedRAMP controls relate not to a company’s cybersecurity program writ large, but to the specific cloud product being certified: *e.g.*, whenever the controls specify a requirement for “the information system,” the reference is to the cloud product being certified, not the company’s corporate network. DS ¶¶ 53-54. Accordingly, even if Ms. Pierce’s “preliminary review” were a reliable record of whether SolarWinds could meet FedRAMP requirements—and it is plainly not—it would not be probative of whether SolarWinds was implementing the much different, more basic practices set forth in the Security Statement.

Indeed, the SEC has cited only one FedRAMP control that roughly maps onto a representation in the Security Statement, about following the principle of least privilege. GR ¶¶ 64-

66.²¹ Ms. Pierce marked it as a control SolarWinds “may have” in place, commenting: “This is included in the Access/Security Guidelines document. An audit that this is in place has never been performed.” DS ¶ 68. Besides being irrelevant to the Security Statement—which says nothing about whether SolarWinds ever “audited” its compliance with the principle of least privilege—the comment is demonstrably wrong: SolarWinds *did* perform such audits, including internal audits *that the SEC itself has cited*, e.g., AC ¶ 188, as well as in user access reviews the Company conducted on a quarterly basis and in audits by multiple outside audit firms during the Relevant Period. JS ¶¶ 96-97; DS ¶ 69. This only underscores why Ms. Pierce’s “preliminary review” is not reliable evidence in the first place. *See Dalberth v. Xerox Corp.*, 766 F.3d 172, 184 (2d Cir. 2014) (holding comments in internal documents could not raise genuine dispute where direct evidence contradicted the inference plaintiffs sought to draw).

* * *

The SEC’s reliance on these and similar notations, haphazardly plucked from scattered documents, is unavailing. Every single witness with knowledge of the cited documents rejected the SEC’s interpretation of them and explained that they did not contradict anything in the Security Statement.²² Courts do not hesitate to grant summary judgment in light of such unrebutted explanatory testimony. *See, e.g., Tieu*, 717 F. Supp. 3d at 330; *Mirror Worlds Techs., LLC v. Facebook, Inc.*, 588 F. Supp. 3d 526, 552 (S.D.N.Y. 2022) (no genuine dispute where defendant’s director of engineering explained purported discrepancy in technical diagram), *aff’d*, 122 F.4th

²¹ The FedRAMP control states: “The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.” DS ¶ 67.

²² *See* Pre-Mot. Summ. J. Conf. Tr., ECF No. 164, at 13:15-19 (counsel for SEC conceding that “We asked witnesses about these documents. And ... there’s no witness that comes out and says ‘... the SEC is right, you know, this security statement was false.’”).

860 (Fed. Cir. 2024); *Sheridan v. Jaffe*, 1996 WL 345965, at *9 (S.D.N.Y. June 24, 1996) (letter was “not evidence” to resist summary judgment in light of recipient’s “uncontradicted testimony” explaining it); *Vantage Point, Inc. v. Parker Bros.*, 529 F. Supp. 1204, 1213-14 (E.D.N.Y. 1981) (no genuine dispute where defendant’s employee “who was familiar with the company’s procedures” explained meaning of document), *aff’d*, 697 F.2d 301 (2d Cir. 1982); *Jysk Bed’N Linen v. Dutta-Roy*, 787 F. App’x 608, 611 (11th Cir. 2019) (affirming summary judgment where email recipient submitted un rebutted affidavit explaining it); *Self v. Crum*, 439 F.3d 1227, 1236 (10th Cir. 2006) (refusing to draw plaintiff’s asserted inferences from defendant’s notes in light of defendant’s testimony explaining them).²³

The SEC cannot resist summary judgment merely by invoking a vague intention to attack witnesses’ credibility. “If the most that can be hoped for is the discrediting of defendants’ denials at trial[,] no question of material facts is presented.” *Fernandez v. China Ocean Shipping, (Grp.) Co.*, 312 F. Supp. 2d 369, 378 (E.D.N.Y. 2003), *aff’d*, 94 F. App’x 866 (2d Cir. 2004); *see also Dowd v. IRS*, 776 F.2d 1083, 1084 (2d Cir. 1985) (affirming summary judgment where “appellants had deposed every employee with firsthand knowledge of the records, and all uniformly denied [allegations regarding those records]”); *USA Certified Merchs., LLC v. Koebel*, 262 F. Supp. 2d 319, 334 (S.D.N.Y. 2003) (granting judgment where defendant testified “he had no knowledge” of the alleged fraudulent scheme and “[p]laintiffs produce[d] no evidence to rebut this testimony”); *see also Kidd v. Midland Credit Mgmt., Inc.*, 2019 WL 4736913, at *2 (E.D.N.Y. Sept. 27, 2019)

²³ The SEC fares no better with other documents where it failed to depose their authors at all. Such is the case, for example, with a document the SEC cites titled “MSP Products Security Evaluation,” which the SEC seeks to rely on despite making no effort to depose the authors who wrote it. *See Sheridan*, 1996 WL 345965, at *8 (granting summary judgment where plaintiff “neither deposed [the sender] nor asked [the recipient] about [a critical] letter at his deposition”); *Deng v. 278 Gramercy Park Grp., LLC*, 23 F. Supp. 3d 281, 287-88 (S.D.N.Y. 2014) (same, where opponent failed to seek testimony from transaction participants); *Conn. Indem. Co. v. 21st Century Transp. Co.*, 186 F. Supp. 2d 264, 276 (E.D.N.Y. 2002) (similar).

(“Courts routinely reject attempts by parties to raise an issue of fact on summary judgment solely by challenging the opposing party’s testimony on credibility grounds.”).

The bottom line is that the SEC had *years* to investigate this case and to find evidence to support its claims. If there really were “long-standing, pervasive, systemic, and material” failures to implement the practices in the Security Statement, then why couldn’t the SEC find a single witness to say that? If SolarWinds really granted everyone “admin” rights to sensitive systems, then why couldn’t it find a single employee to testify they unnecessarily received those rights? If SolarWinds really persistently failed to do security testing on its products, then why couldn’t it find a single software developer to testify that a product they worked on went out untested? The SEC cannot excuse this absence of evidence simply by falling back on the same self-serving characterizations of documents alleged in the Amended Complaint, as if discovery never happened. “[U]nless [the plaintiff has] thus far turned up evidence from the defendants or elsewhere supporting their ... theory,” there is no reason to believe that “in the face of defendants’ uncontradicted evidence negating it, trial would give them any greater opportunity to elicit from defendants and their employees evidence tending to prove it.” *Mod. Home Inst., Inc. v. Hartford Accident & Indem. Co.*, 513 F.2d 102, 110 (2d Cir. 1975); see *In re REMEC Inc. Sec. Litig.*, 702 F. Supp. 2d 1202, 1241 (S.D. Cal. 2010) (granting summary judgment where “Plaintiffs have not produced a witness to testify to the truth of the aspersions recited in the complaint”).

C. The SEC Cannot Avoid Summary Judgment by Changing Its Theory of the Case—Especially When the New Theory Makes No Sense

Unable to develop evidence that SolarWinds pervasively failed to implement the Subject Policies, the SEC now essentially seeks to amend its theory of the case. In its Amended Complaint, the SEC assured the Court that “[t]his is not a case about isolated failures,” but rather about

“pervasive” deficiencies.²⁴ Yet, now that those allegations have floundered in discovery, the SEC protests that it does not need to show “there were pervasive deficiencies,” asserting that “[t]he types of major cybersecurity weaknesses experienced by SolarWinds during the relevant period need not materialize many times for them to indicate a *systemic* problem.” SEC Resp. to Defs.’ Req. for Summ. J. Pre-Mot. Conf., ECF No. 162 at 2 (“SEC Pre-Motion Ltr.”). In other words, unable to show “pervasiveness,” the SEC offers a new falsity theory based on the purported “magnitude” of alleged *isolated* failures that this case was allegedly “not ... about.” It is too late for the SEC to raise this substitute legal theory, which amounts to sheer sophistry anyway.

“It is ‘well settled that a Court should not on summary judgment consider factual allegations and legal theories not raised in the complaint.’” *Lopez v. Gap, Inc.*, 883 F. Supp. 2d 400, 413 (S.D.N.Y. 2012) (Engelmayer, J.). This rule prevents securities-fraud plaintiffs like the SEC from changing their theory of why a statement was false or misleading—which would make a dead letter out of Rule 9(b)’s requirement to “plead ... with particularity ... why the statements were fraudulent.” *Novak v. Kasaks*, 216 F.3d 300, 306 (2d Cir. 2000). Thus, for example, in *In re Allergan PLC Securities Litigation*, plaintiffs originally pled falsity on the theory that the defendant had concealed a regulatory determination about its product; but after discovery showed no such determination was ever made, they tried to switch to a theory that the defendant sought to conceal the “extent of regulatory scrutiny” it faced—which the court rejected as different from the theory originally pled. 2022 WL 17584155, at *11, 22 (S.D.N.Y. Dec. 12, 2022), *aff’d*, 2024 WL 677081 (2d Cir. Feb. 20, 2024).

The SEC is attempting a similar switch here. The theory in the Amended Complaint is that

²⁴ AC ¶ 2; *see id.* ¶ 11 (alleging “pervasive cybersecurity problems”); *id.* ¶ 73 (alleging “failures so pervasive in critical areas that they represented systemic problems, and programmatic failures across wide swaths of SolarWinds or even the entire Company”); *see also, e.g., id.* ¶¶ 102, 115, 154, 182, 226 (similar).

SolarWinds failed to implement practices in the Security Statement in a way that was “pervasive,” “systemic,” “routine,” “long-standing,” and “organization-wide.” Those terms denote *frequent* and *widespread* failures, not mere one-off events. “Pervasive” means “present or noticeable in every part of a thing or place.”²⁵ Likewise, “systemic” means “relating to or affecting the whole of a system, organization, etc. rather than just some parts of it.”²⁶ The SEC cannot show “pervasive” or “systemic” failures, so it is trying to save its case by calling isolated events—through *ipse dixit* assertions from its expert—“major” or of “significant magnitude” (whatever that means).

An example helps illustrate. The SEC’s expert, Mark Graff, purports to identify evidence that is “inconsistent” with the Security Statement’s representation about enforcing complex passwords. GR ¶¶ 93(a), 130-134. But he cites only a single password (“solarwinds123”) for a single account on a third-party service—out of many thousands of passwords that would have been used at the Company. Because the account was on third-party infrastructure, SolarWinds could not automatically enforce complexity requirements on the account, but had to rely on individual compliance, which is always subject to human error. DS ¶¶ 110-12. Yet Mr. Graff concludes this one password “is, in and of itself, indicative of a systemic issue” because it was accidentally leaked in a searchable database and because he (erroneously) believes that it could have been used to distribute malicious software if a hacker had found it. GR ¶ 91. That an “incident” of this “*magnitude*” occurred, he says, “indicates” a larger problem. *Id.*

Notably, this “incident” is not even “inconsistent” with the Security Statement, which did not guarantee the complexity of every password any employee used anywhere; rather, it said SolarWinds’ “best practices” were to “enforce the use of complex passwords”—which logically

²⁵ *Pervasive*, Cambridge US English Dictionary, <http://bit.ly/pervas01> (last visited Apr. 25, 2025).

²⁶ *Systemic*, Cambridge US English Dictionary, <http://bit.ly/syst01> (last visited Apr. 25, 2025).

only applies to systems where it is *possible* to enforce the use of complex passwords, unlike the third-party service at issue here. JS ¶¶ 116-17. But even assuming this incident *did* involve a deviation from the Security Statement, and that it *was* “major” in some sense, that still would not support the theory alleged in the Amended Complaint, which is that there were not merely “isolated instances of failing to adhere to a password policy,” but “systemic, organizational-level failures” to do so. The argument that the “magnitude” of a single incident somehow “indicates” systemic or pervasive failures is simply nonsense. Indeed, Mr. Graff acknowledged at his deposition he had no evidence that the use of non-complex passwords “was a frequent problem” at SolarWinds, so obviously this one incident does not “indicate” that it was. DS ¶ 113.²⁷

The same goes for the few other “incidents” Mr. Graff cites as deviations from the Security Statement.²⁸ They cannot establish falsity, because policy statements like those in the Security Statement cannot reasonably be construed to “guarantee” that a firm will “prevent failures in its ... practices.” *ECA*, 553 F.3d at 206. Occasional deficiencies—even if significant in some sense—do not prove those statements false. *See, e.g., In re Citigroup, Inc. Sec. Litig.*, 330 F. Supp. 2d 367, 372, 375 (S.D.N.Y. 2004) (risk management policies not rendered false by failure to manage risk in transactions with Enron, even though alleged failure led to \$1.2 billion in exposure), *aff’d*, 165 F. App’x 928 (2d Cir. 2006); *In re Union Carbide Class Action Sec. Litig.*, 648 F. Supp. 1322, 1323, 1328 (S.D.N.Y. 1986) (statements concerning safety controls not misleading even though alleged safety failures caused “the worst industrial accident in history”).

Any attempt by the SEC to extrapolate pervasive failures from isolated incidents amounts

²⁷ Moreover, Mr. Graff and the SEC greatly overstate the “magnitude” of this incident. The password at issue could not in fact be used to post files for download on SolarWinds’ websites. Nor is there evidence a malicious actor ever actually discovered or used the password. And SolarWinds promptly changed the password upon discovery. DS ¶¶ 114-16.

²⁸ Defendants’ motion to exclude Mr. Graff’s testimony discusses these examples in detail.

to “conjecture as to the true nature of the facts.” *FTC v. Moses*, 913 F.3d 297, 305 (2d Cir. 2019). If the supposed failures were truly “pervasive” as alleged, then the SEC ought to have appropriately “pervasive” evidence—and must proffer it now to avoid summary judgment. “Without corroborating evidence,” such “one-off allegations do not support an inference of the sort of widespread practices necessary to support [a plaintiff’s] theory of falsity” based on alleged pervasive conduct. *Inchen Huang v. Higgins*, 443 F. Supp. 3d 1031, 1053 (N.D. Cal. 2020). Because this is all the SEC can offer, “after years of discovery including dozens of depositions and the production of thousands of documents,” the Court “must grant summary judgment.” *Alpha Lyracom Space Commc’ns, Inc. v. Comsat Corp.*, 968 F. Supp. 876, 892 (S.D.N.Y. 1996), *aff’d*, 113 F.3d 372 (2d Cir. 1997).

D. The SEC Cannot Avoid Summary Judgment by Challenging Representations That Are Not Actually in the Security Statement

The last way the SEC tries to manufacture falsity is by reading representations into the Security Statement that it does not make, but this move fails too.

The SEC relies on this tactic in particular as to secure software development. Again, there is no genuine dispute that SolarWinds regularly performed the practices specifically listed in that section of the Security Statement—vulnerability scanning, penetration testing, regression testing, and product security assessments. JS ¶¶ 144, 146, 148, 150. So the SEC tries to change the subject, alleging that SolarWinds supposedly failed to do “threat modeling.” AC ¶ 123. But the Security Statement says nothing about “threat modeling.” JS ¶ 26. Nor can the SEC read such representations into passing references in the Security Statement to “standard practices” or “best practices,” AC ¶ 113—words that, by themselves, amount to puffery and lack sufficient content to be actionable. *See Plumber & Steamfitters Loc. 773 Pension Fund v. Danske Bank A/S*, 11 F.4th 90, 103 (2d Cir. 2021) (statement that defendant “takes the steps necessary to comply with

internationally recognized standards” inactionable); *ECA*, 553 F.3d at 206 (same with “best practices in risk management techniques”); *Africa v. Jianpu Tech. Inc.*, 2022 WL 4537973, at *9 (S.D.N.Y. Sept. 28, 2022) (same with “steps [defendant] took to promote regulatory compliance” with “best practices”); *In re Austl. & N.Z. Banking Grp. Ltd. Sec. Litig.*, 2009 WL 4823923, at *11 (S.D.N.Y. Dec. 14, 2009) (same).²⁹

The SEC also tries to manufacture a deviation from the Security Statement’s software development representations by faulting SolarWinds for not doing security testing on the Orion Improvement Program (OIP). JS ¶ 199; AC ¶ 131. But the Security Statement only talks about the Company’s development practices for “our products”—*i.e.*, software it sold to customers. DS ¶ 175. OIP was not a SolarWinds “product.” DS ¶¶ 176-77. It was an *internal* application that *SolarWinds* ran on its own systems to collect usage data and analyze product performance. *Id.* A company’s statement that it tests its “products” does not imply anything about testing its internal business applications. By analogy, a judge’s statement that his chambers cite-checks opinions before filing would not say anything about bench memos. *See DeKalb Cnty. Pension Fund v. Allergan PLC*, 2024 WL 677081, at *3 (2d Cir. Feb. 20, 2024) (affirming summary judgment where “the challenged statements ... did not even purport to speak to the [undisclosed issues]”); *Yorkville Advisors*, 305 F. Supp. 3d at 533 (granting summary judgment where “nothing in the [statement] even mentions these terms” that supposedly rendered it false); *Gillis v. QRX Pharma*

²⁹ The SEC’s expert, Mr. Graff, tries to take this invalid tactic even further, reading the Security Statement’s representation that SolarWinds “follows the NIST Cybersecurity Framework” as an open-ended representation that SolarWinds follows “cybersecurity norms and best practices,” Ex. 3 (GR) ¶ 21, and then argues that this was “not the case” by pointing to supposed failures to follow norms and best practices that are nowhere mentioned in the Security Statement, *e.g.*, *id.* ¶ 126-29 (alleging that SolarWinds failed to prevent passwords from being hard-coded into system configuration files). Following the NIST CSF does not mean, however, that one follows any specific norms or best practices. *See supra* at 7. Indeed, Mr. Graff himself acknowledges that “when someone says they’re following the NIST Cybersecurity Framework, you can’t infer from that that they meet any specific controls.” Ex. 3 (GR) ¶ 21; Ex. 50 (Graff Dep.) 107:2-8.

Ltd., 197 F. Supp. 3d 557, 597 (S.D.N.Y. 2016) (Engelmayer, J.) (dismissing claim where “the information which the [complaint] faults defendants for omitting does not contradict the[ir] statements”); *Shenk v. Karmazin*, 868 F. Supp. 2d 299, 306 (S.D.N.Y. 2012) (“Given the fact that [defendants] made very specific promises ... and the fact that they kept those specific promises, no reasonable jury could find” a materially false statement or omission.).³⁰

III. The SEC Cannot Establish Materiality

The SEC’s case separately fails for lack of evidence of materiality. The SEC lacks evidence that “in deciding whether to buy or sell shares of [SolarWinds’] stock,” *Singh v. Cigna Corp.*, 918 F.3d 57, 63 (2d Cir. 2019), “a *reasonable* investor would have viewed the nondisclosed information as having *significantly* altered the total mix of information made available,” *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 44 (2011) (quote marks omitted).

To begin, the SEC has no evidence that investors ever paid attention to the Security Statement or generally investigate the details of companies’ cybersecurity programs. The only evidence on materiality is the testimony of two stock analysts who closely follow SolarWinds and similar stocks. They both testified that, while they seek to collect any information relevant to the investors they advise, they never looked at the Security Statement before this lawsuit or otherwise inquired about the details of SolarWinds’ cybersecurity program during the Relevant Period—because investors never asked about such matters.³¹ See *In re Miller Indus., Inc.*, 120 F. Supp. 2d

³⁰ Similarly, the SEC faults SolarWinds for allowing employees to use their own devices (rather than company-issued laptops) to remotely connect to the company’s network through its VPN—a practice commonly known as “Bring Your Own Device” or “BYOD.” JS ¶ 166; AC ¶¶ 201, 213. But the Security Statement says nothing about SolarWinds’ BYOD practices. While the SEC has pointed to the section addressed to access controls, that paragraph relates only to role-based access controls, *i.e.*, to the processes for assigning access to employees based on their role. The Security Statement says nothing about what *types of devices* employees could use to access the network, which is an altogether different issue. DS ¶¶ 70-73.

³¹ Ex. 51 (Hedberg. Dep.) 170:10-171:5; Ex. 58 (Thill Dep.) 134:10-135:22, 137:6-16.

1371, 1380-81 (N.D. Ga. 2000) (granting summary judgment on materiality where “the consistent practice of the analyst community was to disregard” allegedly misrepresented issue).

As importantly, there is no evidence the sorts of issues the SEC has cited—*e.g.*, a single non-complex password or an audit finding a few improperly configured privileges—would be material to investors. As both analysts testified, investors know such issues arise daily in cybersecurity programs, the very purpose of which is to identify risks to be remediated and areas to be improved.³² It would be absurd and unworkable if merely posting a general description of a cybersecurity program on a website—as companies commonly do³³—thereby obligates a company thereafter to disclose every problem the program encounters in its day-to-day operation. Such a rule would “bury the shareholders in an avalanche of trivial information.” *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 448-49 (1976); *see, e.g., Foley v. Transocean Ltd.*, 861 F. Supp. 2d 197, 211-12 (S.D.N.Y. 2012) (“To ... suggest[] that [the defendant] was under an obligation to divulge specific safety-related information ... , such as audits that had been conducted of rigs or individual safety practices that were in need of improvement, ... would run counter to established precedent refusing to impose a disclosure burden of this type on public corporations ...”); *In re N. Telecom Ltd. Sec. Litig.*, 116 F. Supp. 2d 446, 459 (S.D.N.Y. 2000) (holding that “public disclosure of internal management and engineering problems falls outside the securities laws”).

It is not enough for the SEC to argue that “cybersecurity is inherently important to a company that sells software products.” SEC Pre-Motion Ltr. 3. No law supports such a blanket

³² Ex. 58 (Thill Dep.) 150:7-13 (agreeing that “[n]o company gets security right all the time” and that a good cybersecurity program is “always looking for gaps” even if it has “policies generally in place”); Ex. 51 (Hedberg Dep.) 211:17-21 (agreeing that companies with good cybersecurity programs “regularly are analyzing their own cybersecurity policies for holes or gaps”).

³³ Ex. 51 (Hedberg Dep.) 68:16-69:9 (“I’ve read things like this before on other websites. ... It’s probably not uncommon to see something like this.”); Ex. 58 (Thill Dep.) 133:15-16 (“It’s a statement that’s on virtually every company’s website.”)

rule, which would effectively eliminate materiality as an element for *anything* companies say about cybersecurity—and conversely require them to disclose *everything* about their cybersecurity. Instead, the materiality inquiry focuses on the significance of the specific “nondisclosed information” at issue, *Siracusano*, 563 U.S. at 44—not the general topic of “cybersecurity,” *see ECA*, 553 F.3d at 206 (“While a bank’s reputation is undeniably important, that does not render a particular statement by a bank regarding its integrity per se material.”); *Greenhouse v. MCG Cap. Corp.*, 392 F.3d 650, 656 (4th Cir. 2004) (“[I]f the specific *fact* misrepresented is immaterial, a suit cannot succeed.”).

The SEC cannot point to any specific “nondisclosed information” other than the documents it cites—which, as the unrebutted evidence shows, do not reflect anything more than SolarWinds identifying occasional problems to address or improvements to make. The analysts deposed in the case did not testify—and had no foundation to testify—otherwise. *See, e.g.*, Thill Dep. 143:2-144:22. Indeed, the SEC presented various documents cited in the Amended Complaint to the analysts and tried getting them to opine that they were material, but the analysts made clear they could not even understand what they meant without additional context³⁴—which only goes to show that the documents do not “speak for themselves” as the SEC insists.

Moreover, the only conceivable materiality of cybersecurity deficiencies is that they might mean that the Company was at risk of a cyberattack. But SolarWinds *specifically disclosed that risk to investors*, with risk factors warning that “our systems ... *are vulnerable*” and that serious breaches could occur “[d]espite our security measures.” AC ¶ 240; ECF No. 91-1 (Sept. 21, 2018 Form S-1) at 25. Thus, investors were already on notice to expect vulnerabilities in SolarWinds’ security measures. Evidence that SolarWinds identified such vulnerabilities would be fully

³⁴ *See supra* note 16 and accompanying text.

consistent with those disclosures and would not have “significantly altered the total mix of information” already available to investors. *See In re Marriott Int’l, Inc.*, 31 F.4th 898, 903 (4th Cir. 2022) (rejecting claim based on website data-privacy statements because “Marriott’s risk disclosures to the SEC—the content actually directed to investors—specifically warned that the company’s systems ‘may not be [sufficient]’”); *In re Intel Corp.. Sec. Litig.*, 2019 WL 1427660, at *11 (N.D. Cal. Mar. 29, 2019) (rejecting claim based on touting security features given, *inter alia*, “the risk warnings about security vulnerabilities in Intel’s SEC filings”); *In re Heartland Payment Sys., Inc. Sec. Litig.*, 2009 WL 4798148, at *5 (D.N.J. Dec. 7, 2009) (rejecting claim based on statement emphasizing company’s “high level of security,” given that “the cautionary statements in the Form 10-K—warning of the possibility of a breach and the consequences of such a breach—make clear that Heartland was not claiming that its security system was invulnerable”).

IV. The SEC Cannot Establish Scienter or Negligence

To survive summary judgment on its fraud claims, the SEC must proffer evidence that the Security Statement was made with scienter—“‘a mental state embracing intent to deceive, manipulate, or defraud’ investors.” *Boca Raton Firefighters & Police Pension Fund v. Bahash*, 506 F. App’x 32, 39 (2d Cir. 2012). The SEC has exclusively (and arbitrarily) targeted Mr. Brown with its scienter allegations. But there is no evidence from which a reasonable jury could conclude that Mr. Brown ever harbored any intent to deceive investors; indeed, the notion that he sought to do so through publishing the Security Statement makes no sense against the facts.

The SEC has sought to frame the question of scienter as simply a question of whether Mr. Brown knew or recklessly disregarded that the Subject Policies were false. There is no evidence that he did—but that is not the relevant question to begin with. Evidence of scienter, even on a recklessness theory, must pertain to the risk of *misleading investors*, not merely the risk that

statements were false. “The key question ... is not whether defendants had knowledge of certain undisclosed facts, but rather whether defendants knew or should have known that their failure to disclose those facts ‘presented a danger of misleading buyers or sellers [of securities].’” *City of Dearborn Heights Act 345 Police & Fire Ret. Sys. v. Waters Corp.*, 632 F.3d 751, 758 (1st Cir. 2011); *see also City of Philadelphia v. Fleming Cos.*, 264 F.3d 1245, 1264 (10th Cir. 2001) (same); *SEC v. Patty*, 891 F.2d 295, 295 (9th Cir. 1989) (similar); *Schlifke v. Seafirst Corp.*, 866 F.2d 935, 946 (7th Cir. 1989); *Teamsters Loc. 445 Freight Div. Pension Fund v. Dynex Cap. Inc.*, 531 F.3d 190, 197 (2d Cir. 2008) (requiring “a compelling motive to mislead investors”). The charge is *securities* fraud, after all. Thus, the ultimate issue on summary judgment “is whether the evidence, taken as a whole, could support a finding by a reasonable juror that defendants acted with the intent to deceive, manipulate, or defraud investors.” *In re N. Telecom Ltd. Sec. Litig.*, 116 F. Supp. 2d 446, 462 (S.D.N.Y. 2000).

There is no evidence—or even a coherent storyline—that Mr. Brown ever thought about investors in connection with the Security Statement, let alone consciously disregarded any risk of misleading them. The Security Statement was directed to SolarWinds’ *customers*, not its investors. JS ¶¶ 27-30. When it was published in November 2017, SolarWinds did not even *have* public investors; the Company’s IPO was not yet planned and did not occur until nearly a year later. JS ¶ 25. And Mr. Brown did not hold any executive position or investor-facing role in any event. JS ¶ 17. These facts are fundamentally incompatible with the idea Mr. Brown intended the Security Statement to mislead investors or consciously disregarded the risk that it would. *See N. Telecom*, 116 F. Supp. 2d at 463 (granting summary judgment where the individual defendants “had no reason to make the alleged misrepresentations or delay disclosure of material information”); *Yorkville*, 305 F. Supp. 3d at 513 (same, where SEC’s motive theory was “not supported by the

circumstances in existence at the time, and, in turn, fails for purposes of establishing scienter”); *Gross v. GFI Grp., Inc.*, 310 F. Supp. 3d 384, 395 (S.D.N.Y. 2018) (same, because “even under [a recklessness] standard, a plaintiff must establish that a material benefit could have been obtained through the misstatement”), *aff’d*, 784 F. App’x 27 (2d Cir. 2019).³⁵

Besides, there would have been no point in trying to deceive investors about SolarWinds’ security measures. When SolarWinds eventually went public, it specifically warned investors that it was vulnerable to cyberattack—“despite” those measures. ECF No. 91-1 at 25. Mr. Brown thus had no reason to try to mislead investors that the Company’s security measures would protect the Company from attack (which the Security Statement never said anyway). The Company’s risk disclosures specifically disclaimed any such assurance. *See City of Coral Springs Police Officers’ Ret. Plan v. Farfetch Ltd.*, 565 F. Supp. 3d 478, 490 (S.D.N.Y. 2021) (that defendants “intentionally put the public on notice of these risks related to their business model strongly negates an inference that they were acting recklessly or consciously to ‘deliberately hide’ them”).

Further, Mr. Brown did not even write the Security Statement. JS ¶¶ 32, 37. There is no evidence, for example, that Mr. Brown prepared the content and simply put in whatever he thought would sound most reassuring (whether to customers or investors). The Security Statement was instead drafted by Mr. Quitugua, who compiled it from preexisting, already vetted answers to

³⁵ None of this is to deny that a statement on a company’s website can, in theory, lead to securities liability. But the fact that a statement was not directed to investors undermines any argument that it was made with intent to mislead investors. Notably, cases imposing securities liability for statements on web pages do not concern customer-directed product webpages like the Security Statement, but rather involve websites and statements clearly aimed at investors. *See SEC v. Enters. Sols., Inc.*, 142 F. Supp. 2d 561, 577 (S.D.N.Y. 2001) (“At the time ESI posted the website, it had not sold any products and it had no customers. ... [I]ts limited operations were funded solely by sales of stock and loans from investors.”); *SEC v. Riel*, 282 F. Supp. 3d 499, 519 (N.D.N.Y. 2017) (“On the REinvest Website, Defendant Riel implied that REinvest could provide investors with high return rates through its investments[.]”); *SEC v. Terry’s Tips, Inc.*, 409 F. Supp. 2d 526, 533 (D. Vt. 2006) (“Terry’s Tips represents, in numerous locations on its website, that its [trading] strategies can be expected to achieve outstanding performance returns [on investment].”).

customer questions that had been in use since before Mr. Brown arrived. JS ¶ 32. Mr. Brown made no significant changes to Mr. Quitugua’s draft, which was also reviewed and approved by Mr. Brown’s supervisors, Ms. Johnson and Mr. Kim, along with SolarWinds’ Legal Department. JS ¶¶ 34-37. Not only does Mr. Brown’s lack of authorship of the document make it implausible that he intended it as a vehicle for deception, but given all the knowledgeable people who reviewed and assented to its content, the idea that it was published recklessly or negligently is fanciful. *See SEC v. Ginder*, 752 F.3d 569, 576 (2d Cir. 2014) (holding that “[n]o reasonable juror could have found” liability under negligence theory where “legal and compliance teams—and [employee]’s supervisors—all approved of his practices”); *SEC v. Shanahan*, 646 F.3d 536, 544 (8th Cir. 2011) (“Depending on others to ensure the accuracy of disclosures ... is not severely reckless conduct[.]”); *REMEC*, 702 F. Supp. 2d at 1242 (granting summary judgment on scienter where defendant’s “budgets were prepared by many employees within the company” and “compile[d]” in a “‘bottoms-up’ procedure [so] that management did not have the opportunity to falsify the budget numbers”).³⁶

In the face of these undisputed facts militating against scienter, the SEC would need powerful evidence to make sense of its story—that, while SolarWinds was still private, Mr. Brown used a customer-facing statement that he did not draft, and that his supervisors had to approve, to deceive investors about the Company’s cybersecurity measures in advance of a then-unplanned

³⁶ Moreover, the Security Statement was also subject to verification by customers—who always could, and sometimes did, demand more information than what the Security Statement provided—as well as outside auditors—who audited some of the very practices that the Security Statement described. These facts, too, make it implausible to believe that Mr. Brown knew the Security Statement to be false but published it anyway—for he would have known that any deceptive statements were likely to be caught. *See Shields v. Citytrust Bancorp, Inc.*, 25 F.3d 1124, 1130 (2d Cir. 1994) (finding no scienter where there was no motive and opportunity to deceive given that truth would have been soon discovered: “It is hard to see what benefits accrue from a short respite from an inevitable day of reckoning.”).

IPO that would not occur until nearly a year later, at which point the Company explicitly warned investors anyway that they could not rely on those measures to protect the Company from attack. Whatever it would take to prove such a far-fetched theory, discovery certainly did not yield it.

To the contrary, Mr. Brown testified that at all relevant times he believed the Subject Policies were true.³⁷ So did Mr. Quitugua, Ms. Johnson, and Mr. Kim.³⁸ And, again, the SEC *concedes* that SolarWinds in fact regularly implemented these policies.³⁹ As discussed above, that fact implies the Subject Policies were true; but *a fortiori*, it implies that Mr. Brown *had reason to believe* they were true. The SEC has no evidence to show that Mr. Brown believed the Subject Policies were “never followed” at all, *Lewy*, 2012 WL 3957916, at *20, or that any failures to implement the Subject Practices were so pervasive and material as to render the Security Statement obviously false, as would be required to raise any inference of scienter. *See Reidinger*, 2021 WL 796261, at *10 (N.D. Cal. Mar. 2, 2021) (no scienter without “ongoing, systematic flaunting of security best practices”); *In re Poseidon Concepts Sec. Litig.*, 2016 WL 3017395, at *15 (S.D.N.Y. May 24, 2016) (no scienter where auditing deficiencies did “not suggest the existence of an audit that was ‘so deficient as to amount to no audit at all’”); *In re Wachovia Equity Sec. Litig.*, 753 F. Supp. 2d 326, 363 (S.D.N.Y. 2011) (no scienter based on internal policy violations where no evidence showed they were “knowingly sanctioned” or the product of “recklessness”); *Medis Inv. Grp. v. Medis Techs., Ltd.*, 586 F. Supp. 2d 136, 143-44 (S.D.N.Y. 2008) (“Where compelling

³⁷ Ex. 46 (Brown Dep.) 142:17-20 (“The security statement, I still believe that was accurate in 2017. It was accurate today. It was accurate throughout the process.”).

³⁸ Ex. 54 (Quitugua Dep.) 157:19-158:6, 325:7-11, 334:1-9, 336:7-12; Ex. 52 (Johnson Dep.) 79:17-82:23, 84:14-85:4, 150:7-12; Ex. 59 (Kim Dep.) 103:24-104:11, 111:19-112:4, 113:5-25, 116:10-117:20.

³⁹ JS ¶¶ 65, 71 (NIST); *id.* ¶¶ 75-76, 93-95 (role-based access controls); *id.* ¶¶ 112, 114, 119, 128 (passwords); *id.* ¶¶ 131, 134-35, 139 (network monitoring); *id.* ¶¶ 146, 148, 150, 152 (secure software development).

circumstantial evidence [of scienter] is required, isolated gray areas are plainly insufficient”), *aff’d*, 328 F. App’x. 754 (2d Cir. 2009).⁴⁰

Nor can the SEC evade its summary judgment burden on scienter and negligence by merely asserting that state of mind is “a quintessential jury issue.” SEC Pre-Motion Ltr. 2. That assertion is as hypocritical as it is wrong: The SEC itself frequently moves for summary judgment in fraud cases when it believes it can establish liability, and “[t]he summary judgment rule would be rendered sterile ... if the mere incantation of intent or state of mind would operate as a talisman to defeat an otherwise valid motion,” *Meiri v. Dacon*, 759 F.2d 989, 998 (2d Cir. 1985). Courts in fact do not hesitate to grant summary judgment where—as here—“based on the lack of material evidence demonstrating scienter or negligence, the SEC is unable to proceed.” *Yorkville*, 305 F. Supp. 3d at 519; *see, e.g., In re Mylan N.V. Sec. Litig.*, 666 F. Supp. 3d 266, 295 (S.D.N.Y. 2023) (granting summary judgment where “no reasonable juror could find that [defendant] consciously or recklessly misled shareholders about its own self-perception of compliance”), *aff’d*, 2024 WL 1613907 (2d Cir. Apr. 15, 2024); *In re Oracle Corp. Sec. Litig.*, 627 F.3d 376, 391 (9th Cir. 2010) (affirming summary judgment because “viewing the totality of the information available to [defendant’s employee] at the time he made the statement, a jury could not reasonably conclude that he had knowledge of facts tending seriously to undermine its accuracy”); *Geffon v. Micrion Corp.*, 249 F.3d 29, 36 (1st Cir. 2001) (affirming summary judgment because “the evidence does not support a finding that defendants *knew* the statements would materially mislead the investing

⁴⁰ For similar reasons that the SEC cannot show scienter, it cannot show negligence either: The undisputed evidence that SolarWinds routinely implemented the Subject Policies implies that it was reasonable for Mr. Brown to believe that the Subject Policies were true. *Yorkville*, 305 F. Supp. 3d at 519; *Ginder*, 752 F.3d at 576 (granting judgment as a matter of law where SEC failed “to present any evidence that the defendant violated an applicable standard of reasonable care”); *Karp v. First Conn. Bancorp, Inc.*, 535 F. Supp. 3d 458, 473 (D. Md. 2021) (granting summary judgment on Exchange Act § 14(a) claim where plaintiff failed to establish negligence), *aff’d*, 69 F.4th 223 (4th Cir. 2023).

public”); *REMEC*, 702 F. Supp. 2d at 1238 (granting summary judgment where “[d]espite their impressive stack of exhibits ... Plaintiffs have not produced evidence sufficient to raise a question of fact of an intent to deceive”).

V. The SEC Cannot Establish a Connection with a Securities Transaction

Finally, the SEC cannot even establish the requisite connection with a security transaction in this case. Sections 10(b) and 17(a) extend only to fraud “in connection with” the purchase, sale, or offer of securities.⁴¹ “Typically, a plaintiff satisfies the ‘in connection with’ requirement when” an identifiable victim of the fraud “bought or sold a security in reliance on misrepresentations as to its value.” *Charles Schwab Corp. v. Bank of Am. Corp.*, 883 F.3d 68, 96 (2d Cir. 2018). In less typical cases, the SEC can establish the requisite connection where the “fraud coincided with the sales [of securities] themselves.” *SEC v. Zandford*, 535 U.S. 813, 820 (2002). The evidence does not support any sufficient connection.

The SEC cannot establish the typical connection because, unlike “every securities case in which [the Supreme] Court has found a fraud to be ‘in connection with’ a purchase or sale of a security,” the SEC cannot point to any actual “victim who took, tried to take, or maintained an ownership position in the statutorily relevant securities through ‘purchases’ or ‘sales’ induced by the fraud.” *Troice*, 571 U.S. at 388-89. Indeed, the SEC has not identified a single investor who even read the Security Statement, let alone purchased SolarWinds’ stock based on it.⁴²

⁴¹ Courts treat the “in” language of Section 17(a) and “in connection with” language of the Securities Litigation Uniform Standards Act, Section 10(b), and Rule 10b-5 as interchangeable, and use caselaw interpreting them accordingly. *See United States v. Naftalin*, 441 U.S. 768, 773 n.4 (1979); *Chadbourne & Parke LLP v. Troice*, 571 U.S. 377, 387-88 (2014).

⁴² To be clear, the SEC (unlike private plaintiffs) need not prove reliance as a separate element; but it *does* have to prove the “in connection with” element. And, while actual reliance is commonly how the element is proven, the SEC cannot do so here. *Cf. SEC v. Infinity Grp. Co.*, 993 F. Supp. 324, 329 (E.D. Pa. 1998) (SEC satisfied connection element with testimony from actual investors who “reviewed [false] materials and relied on them in making investment with the company”),

Nor can the SEC establish that the purported fraud and securities transactions coincided. “For the fraud to ‘coincide’ with a securities transaction, a claim must ‘necessarily allege,’ ‘necessarily involve,’ or necessarily ‘rest on’ the purchase or sale of securities.” *D’Addario v. D’Addario*, 75 F.4th 86, 96 (2d Cir. 2023). That is, “the fraud itself must be ‘integral to the purchase and sale of the securities in question,’” as opposed to being “merely incidental or tangentially related.” *Leykin v. AT & T Corp.*, 423 F. Supp. 2d 229, 241 (S.D.N.Y. 2006), *aff’d*, 216 F. App’x 14 (2d Cir. 2007); *see Troice*, 571 U.S. at 397 (no sufficient connection where securities transactions “constituted no relevant part of the fraud but were rather incidental to it”); *see SEC v. Morgan*, 2019 WL 2385395, at *8 (W.D.N.Y. June 5, 2019) (no connection where “the SEC has not presented any evidence to support the conclusion that the alleged Eden Square scheme coincided with any particular sale of securities”); *SEC v. Mahabub*, 343 F. Supp. 3d 1022, 1049 (D. Colo. 2018) (rejecting mere temporal coincidence, and instead requiring “a showing that [defendant] knew or should have known that his representation would be communicated to investors”), *aff’d*, 32 F.4th 902 (10th Cir. 2022).

No evidence shows any necessary relationship between the purported fraud here—making the Security Statement—and a purchase, sale, or offer of securities. Instead, the undisputed record shows that the Security Statement had nothing to do with securities transactions. It was made by a private company to address customer inquiries about cybersecurity, and merely continued to be used for that purpose when SolarWinds much later happened to conduct an IPO. JS ¶¶ 25-39. That mere (partial) temporal coincidence between “independent events” does not suffice. *Zandford*, 535 U.S. at 820; *see Howard v. Arconic Inc.*, 395 F. Supp. 3d 516, 539 (W.D. Pa. 2019) (“product

aff’d, 212 F.3d 180 (3d Cir. 2000); *United States v. Shelton*, 784 F. App’x 934, 939 (6th Cir. 2019) (connection requirement satisfied by showing misrepresentation was material to particular investors); *cf. SEC v. Pirate Inv. LLC*, 580 F.3d 233, 244 (4th Cir. 2009) (examining connection element in SEC action).

brochures” published on defendant’s website lacked connection because “[t]he goal of the brochures is to persuade a customer to purchase Arconic’s products, not its stocks” and “[t]he brochures are not directed at the financial community”); *Lindblom v. Mobile Telecomms. Techs. Corp.*, 985 F. Supp. 161, 164 (D.D.C. 1997) (no connection where defendant “was not selling stock. It was selling—or attempting to sell—a paging system”); *Hemming v. Alfin Fragrances, Inc.*, 690 F. Supp. 239, 244-45 (S.D.N.Y. 1988) (no connection for magazine advertisement that “concern[ed] Glycel’s qualities as a skin care treatment, not as an investment choice”: “Although an investor might read these promotional materials, the brochure and pamphlet are geared to consumers of a product, not investors in a corporation.”).

Although the connection requirement is construed “flexibly to effectuate its remedial purposes” of protecting securities markets and investors, the Supreme Court has warned that it “must not be construed so broadly as to convert every common-law fraud that happens to involve securities into a violation of” federal securities law. *Zandford*, 535 U.S. at 820. Defendants are aware of no court that has imposed securities fraud liability based on such an attenuated connection to securities as the record shows here. There is no reason why this Court should do so.

CONCLUSION

For the foregoing reasons, Defendants are entitled to summary judgment on all claims.

Dated: April 25, 2025

Respectfully submitted,



Serrin Turner

Matthew Valenti

Nicolas Luongo

LATHAM & WATKINS LLP

1271 Avenue of the Americas

New York, NY 10020

Telephone: (212) 906-1200

Facsimile: (212) 751-4864

serrin.turner@lw.com

matthew.valenti@lw.com

nicolas.luongo@lw.com

Sean M. Berkowitz (*pro hac vice*)

LATHAM & WATKINS LLP

330 N. Wabash, Suite 2800

Chicago, IL 60611

Telephone: (312) 876-7700

Facsimile: (617) 993-9767

sean.berkowitz@lw.com

*Counsel for Defendants SolarWinds Corp. and Timothy
G. Brown*

CERTIFICATE OF SERVICE

I hereby certify that on April 25, 2025, I electronically filed the foregoing document with the Court via CM/ECF, which will automatically send notice and a copy of same to counsel of record via email.


Serrin Turner