No. 21-1802

In the United States Court of Appeals for the Fourth Circuit

In re: Marriott International, Inc.

CONSTRUCTION LABORERS PENSION TRUST FOR SOUTHERN CALIFORNIA,
Plaintiff-Appellant,

v.

MARRIOTT INTERNATIONAL, INC., et al.,
*Defendant-Appellee*s.

On Appeal from the United States District Court for the District of Maryland, Greenbelt Division
(No. 8:19-cv-00368) (The Hon. Paul W. Grimm)

BRIEF OF AMICUS CURIAE THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA IN SUPPORT OF APPELLEES

TARA S. MORRISSEY
PAUL LETTOW
U.S. CHAMBER LITIGATION CENTER
1615 H Street NW
Washington, DC 20062
(202) 463-5747

JUDSON O. LITTLETON
DANIEL J. RICHARDSON
SULLIVAN & CROMWELL LLP
1700 New York Avenue NW
Washington, DC 20006
(202) 956-7500
littletonj@sullcrom.com

RULE 26.1 CORPORATE DISCLOSURE STATEMENT

The Chamber of Commerce of the United States of America ("Chamber") is a non-profit, tax-exempt organization incorporated in the District of Columbia. The Chamber has no parent corporation, and no publicly held company has 10 percent or greater ownership in the Chamber.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases:

Statutes:

Regulations:

Other Authorities:

INTEREST OF THE *AMICUS CURIAE*

The Chamber is the world's largest business federation. It represents approximately 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members in matters before Congress, the Executive Branch, and the courts. To that end, the Chamber regularly files *amicus curiae* briefs in cases that raise issues of concern to the nation's business community. Many of the Chamber's members are companies subject to U.S. securities laws and may be adversely affected if the Court adopts Plaintiff's theories of liability here.[1]

[1] The Chamber affirms that no party or counsel for any party authored this brief in whole or in part and that no one other than the Chamber, its members, or its counsel contributed any money that was intended to fund the preparation or submission of this brief. The parties have consented to this filing.

INTRODUCTION

As Marriott aptly demonstrates, the district court correctly dismissed all of Plaintiff's claims, which seek to convert a company's victimization in a criminal cyberattack into liability for securities fraud. While all of Plaintiff's arguments on appeal lack merit, the Chamber submits this brief to explain why one of Plaintiff's theories of liability in particular misunderstands the law and would have a substantial negative impact on public companies *and* their investors. Specifically, Plaintiff impermissibly seeks to hold a company liable for securities fraud for doing exactly what federal law requires: candidly and truthfully discussing the future risks confronting its business.

The factual context of this case—a securities class action filed in the immediate wake of a major cyberattack—makes it all the more important that these claims be rejected. Cybersecurity threats are ubiquitous in the public and private sectors. Every day, firms large and small face a growing number of sophisticated actors who aim to disable their systems or steal private information. These attacks impose massive costs. *See* IBM, *Costs of a Data Breach Report* 5 (2020) (IBM Report), https://tinyurl.com/IBMDataReport (finding that the average cost of a data breach is $3.86 million). As a result, many public companies now

appropriately disclose cybersecurity risks to investors as one of the principal risks to their businesses, explaining how an attack could destabilize operations, weaken consumer confidence, and hurt the bottom line.

Marriott is one of those companies. For years, it candidly disclosed the risk that a cybersecurity incident would pose to its operations, informing investors that "[c]yber-attacks could have a disruptive effect on our business," and that "[a] significant theft . . . of customer, employee, or company data could adversely impact our reputation and could result in remedial and other expenses, fines, or litigation." J.A. 785. Then, in November 2018, Marriott discovered that a breach of its Starwood guest reservation database had compromised the personal information of over 380 million people. The company promptly notified affected customers and disclosed the breach to the public. And it updated its risk disclosures to investors to acknowledge that "[l]ike most large multinational corporations, we have experienced cyber-attacks, attempts to disrupt access to our systems and data, and attempts to affect the integrity of our data." J.A. 1354-1355.

Yet Plaintiff claims that, through these risk disclosures, Marriott committed securities fraud. Why? Because in the course of discussing the

risk posed by cybersecurity threats, the company did not also provide the general public with internal information detailing its vulnerabilities to a cyberattack.

The most fundamental problem with this theory is that it seeks to hold a company liable for making true statements. Consistent with regulatory requirements governing every public company, Marriott's risk disclosures were forward-looking assessments of the serious threat that cyberattacks posed to the company. In discussing that risk, Marriott had an obligation to be truthful and not misleading. Here, it clearly discharged that obligation, and Plaintiff does not seriously argue otherwise. Instead, Plaintiff's theory boils down to the contention that if Marriott was aware of any additional detail relevant to its current cybersecurity risk profile, the company had to disclose that detail or else face securities fraud liability. But nothing in the securities laws requires companies making concededly accurate assessments of future risks to simultaneously disclose all internal information reflecting how vulnerable they may be to those risks.

Plaintiff's theory would also leave courts and public companies at a loss to figure out what underlying information must accompany a risk disclosure, forcing companies to disclose ever-expanding amounts of information to

avoid securities fraud liability. That would ultimately harm investors, who would be required to sift through volumes of risk-related information rather than the "clear and concise summary" of risks that the securities laws require. *See* SEC, Securities Offering Reform, 70 Fed. Reg. 44,721, 44,786 (Aug. 3, 2005).

ARGUMENT

I. Marriott's Risk Disclosures Are Not Actionable

Federal law requires public companies to include a separate section in certain securities filings that discusses the material "risk factors" facing their businesses. 17 C.F.R. § 229.105. These risk disclosures may implicate every aspect of a firm's operations. In recent years, the growing threat of cyberattacks has led more companies to candidly discuss cybersecurity risks in these disclosures. Here, Marriott assessed the risks that a future cyberattack could pose to its operations and shared that assessment with investors. That is precisely what public companies like Marriott are required to do. Contrary to Plaintiff's theory, they are under no additional obligation to flood the market with all information that may bear on their assessments of (and vulnerabilities to) future risk in order to make those disclosures not misleading.

A. Risk Disclosures Touch on Every Facet of a Business's Operations, Including the Growing Threat of Cyberattacks

Public companies must provide investors with "a discussion of the material factors that make an investment in the [company] speculative or risky." 17 C.F.R. § 229.105. These risk disclosures were first required for annual and quarterly reports in 2005. In adopting this requirement, the SEC instructed companies "to provide investors with a clear and concise summary of the material risks" facing their business, believing that those disclosures would "further enhance the contents of Exchange Act reports and their value in informing investors and the market." 70 Fed. Reg. at 44,786. The SEC again stressed the need for focused and succinct assessments when revamping these regulations just last year, reiterating "the importance of organized and concise risk factor disclosure." SEC, Modernization of Regulation S-K Items 101, 103, and 105, 85 Fed. Reg. 63,726, 63,745 (Oct. 8, 2020). The requirement that companies disclose future risks reflects the central insight that "forward-looking statements provide valuable information for investors in the securities marketplace." *Xia Bi* v. *McAuliffe*, 927 F.3d 177, 183 (4th Cir. 2019).

Consistent with this principle and the SEC's expectations, businesses use these risk disclosures to advise investors of how future, contingent

events may negatively impact their operations. A single company may discuss more than a dozen risks in a single filing, ranging from long-term concerns like industry regulation to emergent issues like the Covid-19 pandemic. *See, e.g.*, Mastercard Incorporated, 2020 Annual Report on Form 10-K ("[M]easures to try to contain the virus . . . may further impact our workforce and operations."). And these risk disclosures often touch on every aspect of a company's operations. *See, e.g.*, Ford Motor Company, 2020 Annual Report on Form 10-K (discussing, among others, the risks associated with "pandemics such as Covid-19," "the successful execution of its [business] Plan," "operational systems . . . affected by cyber incidents," "production . . . disrupted by labor issues," and "Ford's ability to attract and retain talented, diverse, and highly skilled employees").

Few risks are more prominent and ubiquitous today than cybersecurity. Nearly every company has experienced some form of cyberattack. *See* James A. Lewis et al., *The Hidden Costs of Cybercrime*, Ctr. for Strategic & Int'l Stud. 4 (Dec. 2020) (Hidden Costs), https://tinyurl.com/CSISCybercrime (noting that in a survey of more than 1,500 companies, "only 4% claimed that they did not experience any sort of cyber incident in 2019"). A recent study estimates that the costs of

cybercrime grew by more than 50% between 2018 and 2020, *id.* at 3, while another pegs the "total value at risk from cybercrime" at a staggering $5.2 trillion over the next five years, Kelly Bissell et al., *The Cost of Cybercrime*, Accenture 14 (March 2019) (Cost of Cybercrime), https://tinyurl.com/AccentureCybercrime. The nature of this threat is constantly evolving: recent cyberattacks have sought not only to steal data but to hold it hostage or destroy it altogether, and present-day "cybercriminals are adapting their methods" by increasingly exploiting "malicious insiders" within a firm. *Id.* at 6. *See also* GAO WatchBlog, *Ransomware—Holding IT Systems and Data Hostage* (June 30, 2021), https://tinyurl.com/GAORansomware. At the same time, firms are more dependent than ever on the digital economy to carry out their operations and grow their business. *See* Costs of Cybercrime, at 8. In short, cybersecurity presents a growing and persistent risk to the economy, and one that businesses cannot avoid.

As a result, cybersecurity risk is now a universal topic in securities filings. *Every* Fortune 100 company that files an annual 10-K discusses cybersecurity as a material risk in that document, explaining how a future cyberattack could, among other things, destabilize operations, harm

consumer confidence, or invite regulatory scrutiny. *See* Stephen Klemash, *How Cybersecurity Risk Disclosures and Oversight Are Evolving in 2021*, Ernst & Young 2 (Oct. 4, 2021) (EY Report), https://tinyurl.com/EYRiskDisclosures.

As the gravity of the threat has grown, cyber-related risk disclosures have kept pace. In the last decade, companies' filings have provided more cyber-related risk information and have increasingly explained how that risk implicates other facets of their business, including product functionality and public reputation. *See* Grace F. Johnson, *Examining Cybersecurity Risk Reporting on US SEC Form 10-K*, 4 ISACA Journal 1, 3-5 (2018). Firms are also making cybersecurity a greater priority for their leadership, seeking out cybersecurity expertise for their boards and establishing more channels for management to communicate about those issues. EY Report, at 3. *See also* Deloitte, *Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts* 1 (2016), https://tinyurl.com/DeloitteCyberattack ("The idea that cyberattacks are increasingly likely—and perhaps inevitable—is beginning to take hold among executives and boards.")

Properly understood, the SEC's risk disclosure obligations require companies to disclose truthful assessments of the potential risks confronting

their business in order to allow investors to make informed decisions. But the utility of these disclosures would be compromised by a rule that forces companies to bury investors in information in an effort to avoid liability—in the cybersecurity context, potentially even requiring the disclosure of security vulnerabilities to the same bad actors who threaten companies and their customers.

B. Marriott's Risk Disclosures Would Not Mislead a Reasonable Investor

Securities law imposes no "general duty on the part of a company to provide the public with all material information." *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1432 (3d Cir. 1997). That is true even for material information that "a reasonable investor would very much like to know." *In re Time Warner Inc. Sec. Litig.*, 9 F.3d 259, 267 (2d Cir. 1993). Absent an affirmative duty to disclose, a securities plaintiff basing its claims on the contention that a company impermissibly failed to share information with the public must identify a particular *statement* that was rendered misleading by that omission. *See Matrixx Initiatives, Inc.* v. *Siracusano*, 563 U.S. 27, 44-45 (2011). "Whether a statement is misleading depends on the perspective of a reasonable investor." *Omnicare, Inc.* v. *Laborers Dist.*

Council Constr. Indus. Pension Fund, 575 U.S. 175, 186 (2015) (citation omitted).

Plaintiff's risk disclosure claims fail because no reasonable investor would find Marriott's statements misleading. Plaintiff claims to have been misled in two ways. *First*, it claims that Marriott's risk disclosures were misleading because they failed to "provide investors with information necessary to make an accurate assessment of the true cybersecurity-related risks the Company faced." App. Br. 64. But the information Plaintiff seeks has no bearing on the accuracy of Marriott's *actual statements*. A forward-looking discussion of a specific risk is not misleading solely because it does not also include all information purportedly detailing the company's vulnerability to that risk.

Second, Plaintiff argues that Marriott's risk disclosure left it with a "false impression" of what occurred in the *past*. J.A. 1357. But risk disclosures "are inherently *prospective* in nature." *Bondali* v. *Yum! Brands, Inc.*, 620 Fed. Appx. 483, 491 (6th Cir. 2015). Since a risk disclosure only speaks to the future, a reasonable investor would not read such a statement as a reflection of a firm's current or past condition. And even if such a theory could be viable in some other context, it clearly is not here. As the district

court thoroughly explained, there was no inconsistency between Marriott's statements and the actual situation at the company.

1. A Prospective Risk Disclosure Need Not Discuss All Information Detailing a Company's Vulnerability to That Risk

Plaintiff first argues that Marriott's risk disclosures were misleading because, without every piece of information demonstrating the "vulnerability of Starwood's systems," App. Br. 64, an investor might have underappreciated the future risks facing the company. Such a view would convert the duty to not mislead investors into a duty to provide comprehensive documentation supporting each and every risk disclosed to the public. Securities law imposes no such duty.

"Rule 10b-5 'prohibit[s] *only* misleading and untrue statements, not statements that are incomplete.'" *Emps. Ret. Sys. of R.I.* v. *Williams Cos., Inc.*, 889 F.3d 1153, 1164 (10th Cir. 2018) (quoting *Brody* v. *Transitional Hosps. Corp.*, 280 F.3d 997, 1006 (9th Cir. 2002)). As a result, companies need not "dump all known information with every public announcement." *In re K-tel Int'l, Inc. Sec. Litig.*, 300 F.3d 881, 898 (8th Cir. 2002). For example, a company that says publicly it is considering "any legitimate acquisition proposal" need not disclose that it was already meeting with potential

acquirers, *see Glazer* v. *Formica Corp.*, 964 F.2d 149, 157 (2d Cir. 1992), just as a company that announces a share buyback need not disclose a possible merger affecting the value of those shares, *Brody*, 280 F.3d at 1006. Put simply, "Rule 10b-5 does not contain a 'freestanding completeness requirement' because 'no matter how detailed and accurate disclosure statements are, there are likely to be additional details that could have been disclosed but were not.'" *In re Intuitive Surgical Sec. Litig.*, 65 F. Supp. 3d 821, 836 (N.D. Cal. 2014) (quoting *Brody*, 280 F.3d at 1006).

To succeed here, it is therefore not enough for Plaintiff simply to point to undisclosed information that is *related to* Marriott's cyber-related risks. Plaintiff instead must show that Marriott's specific statements regarding its future risk were inaccurate or misleading. As the district court correctly concluded, the complaint does not come close to making that showing.

Marriott's risk disclosures listed many types of cyberattacks that could affect its operations, including "efforts to hack or breach security measures," "viruses," and "ransomware and other malware." J.A. 825. It then provided a detailed discussion of the possible consequences of such an attack, explaining that "[a] significant theft, loss, loss of access to, or fraudulent use of customer, employee, or company data could adversely impact our

reputation and could result in remedial and other expenses, fines, or litigation." *Id.* There is no dispute that all of these statements are true. Nor does information concerning the "vulnerability of Starwood's systems"—reflected in internal audits, tests conducted by third parties, and reports to Marriott's Board—make those statements regarding the serious future risk of a cybersecurity incident at all misleading.

When Marriott disclosed its assessment of future risks, it had a duty to ensure that those disclosures were truthful and not misleading. It did not take on a duty to provide the investing public with all of the information on which its assessment was based. As the district court recognized, there is nothing inconsistent or misleading about identifying a risk of cyberattacks while possessing information bearing on the firm's vulnerabilities to those attacks. J.A. 1358.

Apart from being wrong on the law, Plaintiff's theory—that a company must disclose all known vulnerabilities to the risks it identifies—has no workable limits and will thus give rise to considerable uncertainty. Would a car company that warns of the risk Covid-19 poses to its operations violate the securities laws by failing to tell investors that an internal study showed low vaccination rates among its employees? Would a manufacturing

company that discusses the risk of supply chain disruptions need to disclose an analyst call informing management of possible labor disputes at a supplier? Plaintiff's theory raises any number of these kinds of questions, but offers no clear answers.

Nothing in the duty to identify material risks or in Section 10(b) requires public companies to attempt to draw these lines. As a district court facing a similar claim recently explained, "[t]o construe this full and complete disclosure requirement so broadly as to require an actor to disclose any and all material information when the actor so much as vaguely or generally references subject matter related to the material information would impose an impossible burden." *Indiana Pub. Ret. Sys.* v. *Pluralsight, Inc.*, 2021 WL 1222290, at *13 (D. Utah March 31, 2021).

Like most every other public company, Marriott recognized that it faces risks from cybersecurity incidents. It thus informed investors of its honest and accurate assessment of the consequences such an incident could have for its business. The mere fact that Plaintiff, with the benefit of hindsight, would have wanted to know about Marriott's past cybersecurity vulnerabilities does not make Marriott's actual risk disclosures misleading. And to suggest that liability is appropriate here just because a breach

eventually occurred amounts to nothing more than an attempt to plead "fraud by hindsight." *Hillson Partners Ltd. P'ship* v. *Adage, Inc.*, 42 F.3d 204, 209 (4th Cir. 1994) (citation omitted).

2. A Prospective Risk Disclosure Would Not Mislead a Reasonable Investor as to a Firm's Past or Present Operations

Plaintiff next argues that Marriott's cybersecurity risk disclosures misled investors as to the *current* state of Marriott's cybersecurity protections. App. Br. 65-68. That theory also fails. Risk disclosures speak to what may happen in a company's future, not its present or its past, and a reasonable investor would not think otherwise. And even if a forward-looking risk disclosure *could* mislead an investor as to the present, that is not what happened here. As the district court recognized, there was no daylight between what Marriott told investors and what actually happened. J.A. 1357.

1. Forward-looking statements differ from representations about the present or past. *See generally Slayton* v. *American Express*, 604 F.3d 758, 765 (2d Cir. 2010) (discussing the PLSRA "statutory safe-harbor for forward-looking statements"). The statement "the Braves may win Game 3 of the World Series" communicates nothing about who is currently winning Game 2. Given that commonsense distinction, no reasonable investor would

consult a forward-looking risk disclosure to understand something about a company's past or current operations. "Risk disclosures . . . are inherently *prospective* in nature. They warn an investor of what harms *may* come to their investment. They are not meant to educate investors on what harms are currently affecting the company." *Bondali*, 620 Fed. Appx. at 491.

This Court has already accepted that sound reasoning. In *ChannelAdvisor*, the plaintiff sued a company for warning about the risk of declining revenue associated with customers "demand[ing] fully fixed pricing terms," without also disclosing that a shift towards fully fixed pricing was already underway. *In re ChannelAdvisor Corp. Sec. Litig.*, 2016 WL 1381772, at *2 (E.D.N.C. April 6, 2016). The district court rejected that argument, reasoning that "it is unlikely that a reasonable investor would, from that cautionary [risk disclosure], infer anything about ChannelAdvisor's current contracts." *Id.* at *6. This Court had no difficulty affirming that decision. *Dice* v. *ChannelAdvisor Corp.*, 671 Fed. Appx. 111 (4th Cir. 2016) (per curiam).

Relying on *Bondali* and *ChannelAdvisor*, the district court here correctly concluded that "[t]o the extent Plaintiff alleges that Marriott's risk disclosures were misleading about its *current* state of cybersecurity, those

allegations fail because the risk factor disclosures are not intended to educate investors about harms currently affecting the company." J.A. 1357. That analysis follows from the basic nature of a forward-looking risk assessment: by definition, Marriott's discussion of risks looming in the future did not require it to rehash the past.

2. Even if a forward-looking risk disclosure could mislead a reasonable investor about a company's current conditions in some circumstance, Marriott's statements here plainly did not do so. Plaintiff argues that Marriott misled investors by "warn[ing] of risks that had already materialized"—here, the risk that Marriott's IT systems "may not be able to satisfy the changing requirements of the payment card industry." App. Br. 65-66. But Marriott's risk disclosures said nothing about whether it (or Starwood) presently complied with any particular standard. Instead, they simply noted the "increasingly demanding" regulatory environment and warned of the risk that the company "may not be able to satisfy" those requirements. J.A. 842-843. As the district court explained, the facts on the ground matched the statements in the risk disclosures: Marriott was actively working to bring the Starwood system into compliance with brand

standards, a process it warned investors "may require significant additional investments or time." J.A. 1357.

As for Plaintiff's contention that Marriott's first risk disclosure following the data breach should have provided more detail about the attack, App. Br. 67, that once again has nothing to do with the truth of what Marriott actually said. It is difficult to understand how Marriott's statement that "we have experienced cyber-attacks" can be considered remotely misleading based on the fact that Marriott had experienced a cyberattack.

At bottom, Plaintiff's "materialized harm" argument rests on the faulty premise that a company commits fraud any time an investor forms a mistaken impression of the company's current affairs after reading a forward-looking risk disclosure. But securities law is focused on specific statements made by a company, not vague impressions a litigant later claims to have gleaned from those statements. That is why securities plaintiffs must "specify each statement alleged to have been misleading" at the outset of their case, 15 U.S.C. §78u-4(b)(1), and why a successful omission claim requires pointing to specific statements that were misleading without the undisclosed information. *Matrixx Initiatives*, 563 U.S. at 44. Here, Marriott's actual statements could not have misled any reasonable investor,

so the district court was right to conclude that those statements cannot subject Marriott to liability.

II. Plaintiff's Approach to Risk Disclosures Would Cause Substantial Harm

Given the breadth of modern risk disclosures—and the importance of candid discussions of future risk—Plaintiff's theory of securities fraud would impose considerable costs on public companies and their investors. According to Plaintiff, any time a company publicly discloses a specific risk, it takes on the obligation to disclose (1) all internal information detailing its vulnerabilities to that risk and (2) any past instances where the warned-of risk actually occurred. On that view, it is hard to imagine a significant corporate incident negatively impacting a business that would not give rise to securities fraud liability.

When companies are doing risk assessment correctly, they identify real risks that have some likelihood of occurring. If (or when) those risks materialize, a plaintiff will always be able to point to some piece of information that, with the benefit of hindsight, supposedly shows that the company understated the risk. Public companies would face an impossible choice: flood the market with all information that anyone might conceivably deem relevant to a description of a risk, or face a follow-on securities fraud

suit after every negative event the company had the foresight to warn investors about in advance.

And investors would be no better off. The Supreme Court has cautioned against adopting standards that "lead management 'simply to bury the shareholders in an avalanche of trivial information—a result that is hardly conducive to informed decisionmaking.'" *Basic Inc.* v. *Levinson*, 485 U.S. 224, 231 (1988) (quoting *TSC Indus., Inc.* v. *Northway, Inc.*, 426 U.S. 438, 448-449 (1976)). Similarly, the SEC's risk disclosure regulations recognize that investors benefit from information that is concise and meaningful. *See* 70 Fed. Reg. at 44,786 (requiring that risk factor disclosures be written in "plain English" for the benefit of investors); 85 Fed. Reg. at 63,742 (updating the risk disclosures regulations "to address the lengthy and generic nature of the risk factor disclosures presented by many registrants"). A rule forcing companies to disclose all information bearing on a risk assessment *and* all past instances where that risk materialized would undercut these objectives and muddy the water for investors.

That rule is impractical in any context, but in the area of cybersecurity, it is potentially harmful. Unlike many other significant risks discussed in companies' risk disclosures, which may result from complex and interrelated

factors, cybersecurity risks are driven largely by the intentional conduct of bad actors. Requiring companies to publicly disclose their vulnerabilities to those risks amounts to forcing them to paint targets on their own backs.

Experience bears this out. After a breach is disclosed, hackers can exploit a vulnerability before it has been corrected. *See* Craig A. Newman, *When to Report a Cyberattack? For Companies, That's Still A Dilemma*, N.Y. Times (March 5, 2018), https://tinyurl.com/NYTNewman ("Going public with news of a cyberattack isn't always an easy call. Doing so can risk tipping off the bad guys."). And many companies that experience cyberattacks soon find themselves victimized again. *See* SEC Commissioner Luis A. Aguilar, *The Need For Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses* (Oct 19, 2014), https://tinyurl.com/SECAguilarStatement; Nicole Sganga & Musadiq Bidar, *80% of Ransomware Victims Suffer Repeat Attacks, According to New Report*, CBSNews.com (June 17, 2021), https://tinyurl.com/CBSNewsReport. In reality, due to the constant and evolving threat of cyberattacks, companies often face so many risks at once that "leaders must decide which [cybersecurity] efforts to prioritize." Jim Boehm et al., *The Risk-Based Approach to Cybersecurity*, McKinsey & Co. (Oct. 8, 2019),

https://tinyurl.com/McKinseyCyberrisk. If firms must document every existing vulnerability when discussing cybersecurity risks with the public, as Plaintiff would have it, they may be exposing weaknesses they lack the time, resources, or ability to resolve or sufficiently mitigate.

Should these disclosures lead to more attacks, customers and employees will also suffer. A recent study found that "[c]ustomers' personally identifiable information (PII) was the most frequently compromised type of record, and the costliest." IBM Report, at 8. All told, 80% of data breaches put customer data at risk—"far more than any other type of record." *Id.* Employee data is frequently compromised as well, *id.* at 18, exposing highly sensitive records like "Social Security numbers and medical information," Hidden Costs, at 14.

Disclosing a cyberattack too soon can also impede law enforcement. That is why the Federal Trade Commission advises businesses affected by a breach to "consult with your law enforcement contact about the timing of [notifications] so it doesn't impede the investigation." FTC, Data Breach Response: A Guide for Business (Feb. 2021). The SEC has likewise recognized this problem, advising companies against "mak[ing] detailed disclosures that could compromise [their] cybersecurity efforts—for

example, by providing a 'roadmap' for those who seek to penetrate a company's security protections." SEC Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166, 8,169 (Feb. 26, 2018). All told, an open-ended disclosure obligation would undermine businesses' efforts to protect their data and customers, law enforcement's ability to do its job, and investors' ability to efficiently obtain information relevant to their investment decisions.

CONCLUSION

The district court correctly rejected Plaintiff's efforts to turn a criminal cyberattack into a securities class action. This Court should affirm the district court's judgment.

Respectfully submitted,

/s/ *Judson O. Littleton*

TARA S. MORRISSEY
PAUL LETTOW
U.S. CHAMBER LITIGATION CENTER
1615 H Street NW
Washington, DC 20062
(202) 463-5747

JUDSON O. LITTLETON
DANIEL J. RICHARDSON
SULLIVAN & CROMWELL LLP
1700 New York Avenue, NW
Washington, DC 20006-5215
(202) 956-7500
littletonj@sullcrom.com

OCTOBER 28, 2021

CERTIFICATE OF COMPLIANCE
WITH TYPEFACE AND WORD COUNT LIMITATIONS

I, Judson O. Littleton, counsel for *amicus curiae* the Chamber of Commerce of the United States of America and a member of the Bar of this Court, certify, pursuant to Federal Rule of Appellate Procedure 32(a)(7)(B), that the attached Brief is proportionately spaced, has a typeface of 14 points or more, and contains 4,643 words.

/s/ *Judson O. Littleton*
JUDSON O. LITTLETON

OCTOBER 28, 2021

CERTIFICATE OF SERVICE

I, Judson O. Littleton, counsel for *amicus curiae* the Chamber of Commerce of the United States of America and a member of the Bar of this Court, certify that, on October 28, 2021, a copy of the attached Brief was filed electronically through the CM/ECF system with the Clerk of this Court. The participants in this case are registered CM/ECF users and service will be accomplished by the CM/ECF system.

s/ *Judson O. Littleton*
JUDSON O. LITTLETON

OCTOBER 28, 2021