No. 21-594

IN THE
Supreme Court of the United States

ALPHABET INC., ET AL.,
Petitioners,

v.

RHODE ISLAND, OFFICE OF THE RHODE ISLAND TREASURER ON BEHALF OF THE EMPLOYEES' RETIREMENT SYSTEM OF RHODE ISLAND,
Respondent.

On Petition for a Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

BRIEF IN OPPOSITION FOR RESPONDENT

JASON A. FORGE
ROBBINS GELLER RUDMAN & DOWD LLP
655 West Broadway
Suite 1900
San Diego, CA 92101
(619) 231-1058

DAVID C. FREDERICK
Counsel of Record
DEREK C. REINBOLD
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W.
Suite 400
Washington, D.C. 20036
(202) 326-7900
(dfrederick@kellogghansen.com)

February 2, 2022

QUESTION PRESENTED

Securities and Exchange Commission rules require public companies to file annual reports that disclose, among other things, the most significant factors that make the securities offering speculative or risky. Companies must update those risk disclosures quarterly to account for any changes. Both the SEC and every circuit court of appeals to consider the issue have held that a company *may*, under certain circumstances, have to disclose past or ongoing cybersecurity incidents to give investors an accurate picture of the present risks in the investment.

The question presented is:

Whether the complaint plausibly alleged that a reasonable investor could find Google's risk disclosures, which offered general assurances of unchanged risks despite specific, newly discovered, and significantly greater ongoing data-security risks, materially misleading such that the issue should be decided by a trier of fact and not by the court as a matter of law.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES, REGULATIONS, AND RULES

OTHER MATERIALS

INTRODUCTION

A scandal at Facebook in early 2018 brought legislative and public attention to cybersecurity. The Facebook scandal led Google to look into its own data security.

What Google found was an ongoing crisis in the Google+ social media network. The company uncovered a software bug that had, for nearly three years, exposed the private information of hundreds of thousands of users to third parties. Google managed to fix this "Three-Year Bug." But its problems had only begun. In its bug hunt, the company had uncovered a broader "Privacy Bug" that rendered additional glitches and data exposures inevitable and uncontainable. To protect its core business from the fallout from these unavoidable exposures, Google decided to shutter Google+, then the fifth-largest social media network in the world, with more active monthly users than Twitter or Snapchat. And to avoid the negative attention Facebook had gotten from its scandal, Google executives decided to conceal the company's bugs and its decision to shut down Google+ from investors and Congress, while reporting that there had been no material changes to their data-security risks.

Months later, the *Wall Street Journal* published an exposé aptly titled "Google Exposed User Data, Feared Repercussions of Disclosing to Public." Lawmakers from both parties condemned the company. And the stock of Google's parent company, Alphabet Inc., nosedived, costing investors who had purchased shares at fraudulently inflated prices billions of dollars.

The Ninth Circuit's decision involved a straightforward application of principles governing which types of risks need to be disclosed. Under this Court's precedent, the court of appeals' judgment is correct on

the merits and its factbound analysis presents no split in authority for this Court to resolve. For their alleged conflict, petitioners can do no better than several unpublished, non-precedential, and primarily district court decisions that are readily distinguishable. In any event, this case is a poor vehicle to address petitioners' proffered question presented because, no matter the outcome, Rhode Island Employees' Retirement System has surviving claims that were not challenged below or in Google's petition.

STATEMENT

A. Statutory and Regulatory Background

1. Congress enacted the Securities Act of 1933 and the Securities Exchange Act of 1934 ("Exchange Act") in response to rampant abuses in the securities industry. An "animating purpose of the Exchange Act [is] to ensure honest securities markets and thereby promote investor confidence." *United States v. O'Hagan*, 521 U.S. 642, 658 (1997). To advance that purpose, Section 10(b) of the Exchange Act forbids the use of "any manipulative or deceptive device or contrivance" "in connection with the purchase or sale of any security." 15 U.S.C. § 78j(b).

Securities and Exchange Commission ("SEC" or "Commission") Rule 10b-5 implements Section 10(b) by prohibiting "(a) . . . any device, scheme, or artifice to defraud, (b) . . . any untrue statement of a material fact or . . . omi[ssion of] a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, [and] (c) . . . any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person." 17 C.F.R. § 240.10b-5. A private plaintiff seeking relief for a violation of Rule 10b-5(b) must show "(1) a material misrepresentation

or omission by the defendant; (2) scienter; (3) a connection between the misrepresentation or omission and the purchase or sale of a security; (4) reliance upon the misrepresentation or omission; (5) economic loss; and (6) loss causation." *Stoneridge Inv. Partners, LLC v. Scientific-Atlanta, Inc.*, 552 U.S. 148, 157 (2008).

The Private Securities Litigation Reform Act of 1995 ("PSLRA") requires that the complaint in a securities-fraud action alleging a material misstatement or omission "specify each statement alleged to have been misleading, [and] the reason or reasons why the statement is misleading," and provide a particularized basis for any allegations made on information and belief. 15 U.S.C. § 78u-4(b)(1). But the PSLRA imposes no heightened pleading standard for allegations that a misstatement or omission was materially misleading. Those allegations are governed by Federal Rule of Civil Procedure 8(a)(2), which requires a civil complaint to have "a short and plain statement of the claim showing that the pleader is entitled to relief."

2. A publicly traded company must file an annual report and three quarterly reports with the SEC. *See* 15 U.S.C. § 78m; 17 C.F.R. § 249.310 (annual reports); *id.* § 249.308a (quarterly reports). An annual report on Form 10-K gives a comprehensive summary of the company's financial performance; quarterly reports on Form 10-Q provide similar information, but in less detail. In its annual report, a company must "provide under the caption 'Risk Factors' a discussion of the most significant factors that make the offering speculative or risky." 17 C.F.R. § 229.503(c) (2017).[1]

---

[1] A substantially similar provision is now codified at 17 C.F.R. § 229.105. *See* Final Rule, FAST Act Modernization and Simplification of Regulation S–K, 84 Fed. Reg. 12,674, 12,702-03 (Apr.

And in its quarterly reports, a company must disclose "any material changes from risk factors as previously disclosed" in the annual report. Final Rule, Securities Offering Reform, 70 Fed. Reg. 44,722, 44,830 (Aug. 3, 2005).

B. Factual History

1. In 2011, Google launched its social network, Google+. ER31 (¶ 31). Google+ would compete with existing social media companies like Facebook and Twitter. And it would operate as a "social layer" across Google's other services (Search, Gmail, YouTube). ER31-32 (¶ 31). For example, users drafting YouTube comments would have to log into their Google+ accounts to post them. ER32 (¶ 32).

Google+ users trusted Google with private data like their birthdates, addresses, occupations, and even relationship histories. ER35 (¶ 37). Google uses that information to sell targeted advertisements. ER26 (¶ 18). User data fuels Google. As one media outlet explained, Google's "financial success hinges on its success to learn about the interests, habits and location of its users in order to sell targeted ads." ER43 (¶ 65).

Because Google depends on the mass collection and aggregation of user data, it depends on users trusting Google to keep their information secure. ER26-27 (¶ 19). The company's former Executive Chairman, Eric Schmidt, emphasized that a breach of this trust, like a significant data exposure, "would be devastat-

---

2, 2019). After the class period here, the SEC amended the risk-disclosure provision to, among other things, "change the standard for disclosure from the 'most significant' risks to 'material' risks." Final Rule, Modernization of Regulation S–K Items 101, 103, and 105, 85 Fed. Reg. 63,726, 63,742-46, 63,761 (Oct. 8, 2020) (codified at 17 C.F.R. § 229.105).

ing." ER27 (¶ 20). In his words, "[W]e're always one mistake away." *Id.*

Google acknowledges the existential risk of data-privacy exposures in its SEC filings. In its 2017 Annual Report, the company warned:

> Privacy concerns relating to our technology could damage our reputation and deter current and potential users or customers from our products and services. . . . If our security measures are breached resulting in the improper use and disclosure of user data, or if our services are subject to attacks that degrade or deny the ability of users to access our products and services, our products and services may be perceived as not being secure, users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure.

ER30 (¶ 27(a), (b)) (emphases omitted). The disclosure then said that "[a]ny systems failure or compromise of our security that results in the release of our users' data" could "seriously harm our reputation and brand" and thus "impair our ability to attract and retain users." *Id.* (¶ 27(d)). Even "unfounded" "[c]oncerns about our practices with regard to the collection, use, disclosure, or security of personal information or other privacy related matters . . . could damage our reputation and adversely affect our operating results." *Id.* (¶ 27(c)).

2. In spring 2018, social media companies' data-security practices came under public scrutiny. News broke that research firm Cambridge Analytica had improperly harvested data from Facebook users to sell targeted political advertisements. ER32 (¶ 33). That revelation dealt a serious blow to Facebook's common stock, which dipped more than 13%, costing Facebook

approximately $75 billion in market capitalization. *Id.* Congressional investigations followed. ER32-33 (¶ 33(a)).

The Facebook revelation led Google to examine its own data privacy more closely. In doing so, the company learned that it had essentially the same security vulnerability as Facebook: an application programming interface, or API, allowed third-party developers to access the private data of Google+ users. ER32-33, ER42 (¶¶ 33(d), 62). Google had failed to detect this bug for more than three years (respondent's complaint calls it the "Three-Year Bug"). And because Google maintained only two weeks of the relevant records, it could not identify how many users' personal information had leaked because of that glitch. ER35-36 (¶¶ 37-38). Google patched the bug in March 2018. ER46 (¶ 73).

That first bug was "just the tip of the iceberg," according to the complaint. *Id.* Google's investigation turned up other "previously unknown, or unappreciated, security vulnerabilities that made additional exposures virtually inevitable." ER36 (¶ 38). (The complaint refers to the Three-Year Bug and other vulnerabilities Google found, collectively, as the "Privacy Bug.")

Google's legal and policy staff prepared a memorandum on these continuing data-privacy issues (the "Privacy Bug Memo"). ER35-36 (¶ 38). That document outlined the company's internal debate about whether it should disclose the security issues to the public. It warned that disclosing the issues likely would trigger "immediate regulatory interest," would lead to Google "coming into the spotlight alongside or even instead of Facebook despite having stayed under the radar throughout the Cambridge Analytica scandal," and would "almost

guarantee[] Sundar [Pichai, Google's CEO,] will testify before Congress." *Id.* In other words, Google learned its data-security risk profile had worsened at the worst time.

Google executives allegedly received and read the memorandum in April 2018. They decided to buy time by concealing the issues it identified. ER41 (¶ 56). Their plan was "to avoid any additional regulatory scrutiny, including having to testify before Congress." ER36 (¶ 40). This plan marked a shift from a professed policy of "disclosure and transparency" to one of "concealment and opacity." ER38, ER42 (¶¶ 47, 60). And because Google could not prevent Google+ data breaches, the executives approved (and concealed) a plan to shut down the consumer side of the platform. At the time, Google+ was one of the largest social media networks in the world, with more monthly active users than either Twitter or Snapchat. ER36 (¶ 41).

Google continued to give the public the same assurances about security and privacy as before. In April 2018, the company filed its quarterly report with the SEC. The report incorporated the risk disclosures from the company's 2017 annual report and said nothing about the Privacy Bug or the related decision to shutter Google+. It instead disclosed that there "ha[d] been no material changes to our risk factors since our Annual Report on Form 10-K for the year ended December 31, 2017." ER37 (¶ 43). The company took the same tack in its July 2018 quarterly report: It again incorporated the 2017 risk factors and affirmed that there had been no material changes to its risks. ER38-39 (¶ 49).

3. In October 2018, the *Wall Street Journal* exposed Google's discovery of Google+'s security vulnerabilities and its decision to conceal them. *See*

Douglas MacMillan & Robert McMillan, *Google Exposed User Data, Feared Repercussions of Disclosing to Public*, Wall St. J. (Oct. 8, 2018). The story reported that "Google exposed the private data of hundreds of thousands of users of the Google+ social network and then opted not to disclose the issue this past spring, in part because of fears that doing so would draw regulatory scrutiny and cause reputational damage." *Id.* It explained how Google had discovered the many data-security issues with Google+ and that the company made "concerted efforts to avoid public scrutiny of how it handles user information, particularly at a time when regulators and consumer privacy groups are leading a charge to hold tech giants accountable for the vast power they wield over the personal data of billions of people." *Id.*

The day the *Wall Street Journal* published its story, Google acknowledged the "significant challenges" the newspaper had uncovered. ER41 (¶ 58). In a blog post, the company admitted to exposing the private data of hundreds of thousands of users and announced it would be shutting down the Google+ social network for consumers. *Id.*

The reaction was swift. Financial press labeled Google's decision not to disclose its bugs a "cover-up" and predicted regulatory scrutiny. ER44 (¶¶ 67-68).

Two days after the *Wall Street Journal* article, Democratic senators wrote to demand an investigation by the Federal Trade Commission. ER41-42 (¶ 59). Their letter noted that, because of the limitations of Google's internal logs, "we may never know the full extent of the damage caused by the failure to provide adequate controls and protection to users." ER42 (¶ 59). Senator Grassley, then Chair of the Senate Judiciary Committee, wrote to Pichai. He complained

that Google had assured him in April 2018 that it maintained robust protection for user data, even though Pichai knew Google+ "had an almost identical feature to Facebook, which allowed third party developers to access information from users as well as private information of those users' connections." *Id.* (¶ 62).

The markets also reacted. The share price for securities in Alphabet Inc., Google's parent company, allegedly fell after the *Wall Street Journal* article – by $11.91 on October 8, $10.75 on October 9, and $53.01 on October 10. ER50 (¶ 82).

4. Just weeks later – and mere hours before Pichai was set to testify before Congress – Google disclosed in a blog post that it had discovered another Google+ bug. ER43 (¶ 64). This bug had exposed user data from 52.5 million accounts, confirming "Google's inability to protect users' personal and private information," according to the complaint. *Id.* In the same post, Google announced it would shut down the consumer Google+ platform four months earlier than first planned. *Id.*

C. Procedural History

1. Respondents are individuals and entities that acquired securities of Alphabet Inc. at inflated prices from April 23, 2018, to October 7, 2018.[2] Shortly after the *Wall Street Journal* article, several plaintiffs filed securities-fraud actions against Alphabet, Google, and the company's senior executives. App. 12a. The district court designated as lead plaintiff respondent State of Rhode Island, Office of the Rhode Island

---

[2] The class period runs from the day Google filed its April 2018 quarterly report to the day before the *Wall Street Journal* published its story. ER22 (¶ 1).

Treasurer on behalf of the Employees' Retirement System of Rhode Island. *Id.*

Rhode Island Employees' Retirement System filed the operative consolidated complaint in April 2019. The complaint alleges statement-based liability under Rule 10b-5(b) and scheme-based liability under Rule 10b-5(a) and (c). ER53 (¶ 95). The complaint also alleges violations of Section 20(a) of the Exchange Act, which imposes joint and several liability on persons in control of "any person liable under any provision" of securities law. 15 U.S.C. § 78t(a).

2. Google moved to dismiss, challenging only the statement-based claims under Rule 10b-5(b) and Section 20(a). App. 36a.

The district court granted Google's motion to dismiss. App. 49a. It characterized Google's ongoing data-security issues with Google+ as a "past problem[]" for which the company already had "implemented a fix," though the complaint alleges the company had patched only the first of many bugs Google had discovered. App. 44a. And the court held that "a remediated technological problem which is no longer extant [need not] be disclosed in the company's future-looking disclosures." *Id.*

The complaint alleges that the first bug was "just the tip of the iceberg" and that other security vulnerabilities remained an existential threat that led Google to decide to shut down Google+ and to conceal its plan to do so. ER45-46 (¶ 73). The district court did not credit these allegations, stating that Google's broader data-security issues "d[id] not appear in the complaint." App. 48a n.1. In fact, the complaint refers to Google's many security issues as the "Privacy Bug," a defined term that appears in 25 of the complaint's 108 paragraphs.

Google had moved to dismiss only the statement-based claims brought under Rule 10b-5(b). But the district court dismissed the whole complaint sua sponte, including the scheme-based claims under Rule 10b-5(a) and (c), with leave to amend. App. 49a. Rhode Island Employees' Retirement System notified the court that it did not intend to amend, so the district court entered final judgment. Dist. Ct. ECF #84.

3. The Ninth Circuit reversed. The court relied on longstanding circuit precedent holding that, in some cases, "[r]isk disclosures that 'speak[] entirely of as-yet-unrealized risks and contingencies' and do not 'alert[] the reader that some of these risks may already have come to fruition' can mislead reasonable investors." App. 24a (quoting *Berson v. Applied Signal Tech., Inc.*, 527 F.3d 982, 985-87 (9th Cir. 2008)) (first alteration added). The court held that "the complaint plausibly alleges that [Google's] warnings in each [quarterly report] of risks that 'could' or 'may' occur is misleading to a reasonable investor when [Google] knew that those risks had materialized." App. 25a.

Google argued that its quarterly reports were not misleading because it had remediated the Three-Year Bug. *Id.* Because that bug "ha[d] already materialized," Google argued it did not need to be disclosed as a future risk. App. 25a-26a. The Ninth Circuit rejected the argument "for several reasons." App. 26a. *First*, because "Google's business model is based on trust," it was not enough for the company just to "plug[] the hole in Google+'s security" from the Three-Year Bug. *Id.* That bug had lasted for three years, but Google could track only two weeks' worth of issues. The company thus could not determine "the scope and impact of the glitch, [which] indicated that there were

significant problems with Google's security controls." *Id.* *Second*, that first bug was not Google's only issue. The memorandum Google prepared had "highlighted additional security vulnerabilities that were so significant that they allegedly led to Google's decision to shut down the Google+ consumer platform." *Id.*

The Ninth Circuit concluded that Google's failure to disclose its data-security issues was materially misleading. It buttressed that conclusion by noting the complaint alleges that the *Wall Street Journal*'s exposé "resulted in a swift stock price decline, legislative scrutiny, and public reaction, all of which support the allegation that the Privacy Bug was material." App. 27a.

The Ninth Circuit then reversed the district court's sua sponte dismissal of the scheme-based liability allegations. It concluded that "Alphabet's motion to dismiss did not target Rhode Island's Rule 10b-5(a) and (c) claims." App. 36a. And it rejected Google's argument that these claims were duplicative of the statement-based liability claims under Rule 10b-5(b). App. 36a-37a.[3]

4. Google petitioned for rehearing and rehearing en banc. The panel unanimously denied the petition for rehearing, and no judge requested a vote for en banc consideration. App. 52a-53a.

---

[3] The Ninth Circuit also held that Google acted with the requisite scienter and reversed the district court's dismissal on those grounds. App. 28a-33a. It also reversed the dismissal of the Section 20(a) claims based on the April 2018 and July 2018 quarterly reports. App. 36a-37a. The petition does not challenge those holdings. The Ninth Circuit affirmed the district court's dismissal of 10 other statements the complaint alleged were materially misleading. App. 33a-36a.

REASONS FOR DENYING THE PETITION

I. THE NINTH CIRCUIT'S DECISION WAS CORRECT

The Ninth Circuit rightly decided Rhode Island Employees' Retirement System plausibly had alleged that Google's quarterly report risk disclosures were materially misleading. That decision properly reserved ultimate decision on that fact-intensive issue for the factfinder. Below – as here – Google pressed a categorical rule that risk disclosures related to past events *never* can be materially misleading to reasonable investors. The Ninth Circuit rejected such a rule as out of step with the contextual analysis this Court uses to consider securities claims. That correct decision presents no issue meriting this Court's review.

A. A Contextual Rule Governs Whether Statements Or Omissions Are Materially Misleading

1. Companies must disclose the material facts necessary to make their statements, "'in the light of the circumstances under which they were made, not misleading.'" *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 37 (2011) (quoting 17 C.F.R. § 240.10b-5(b)). To determine whether a statement or omission is materially misleading "requires delicate assessments of the inferences a 'reasonable shareholder' would draw from a given set of facts and the significance of those inferences to him." *TSC Indus., Inc. v. Northway, Inc.*, 426 U.S. 438, 450 (1976). This analysis is "'fact-specific,'" *Matrixx*, 563 U.S. at 43 (quoting *Basic Inc. v. Levinson*, 485 U.S. 224, 236 (1988)), and generally a job "for the trier of fact," *TSC Indus.*, 426 U.S. at 450. Only when "reasonable minds cannot differ" is this question "appropriately resolved as a matter of law." *Id.* (internal quotation marks omitted).

The materially misleading analysis involves two questions that each require the trier of fact to consider the full context available to an investor. The first question is whether a statement is misleading. The answer necessarily "depend[s] on the circumstances" under which the speaker made the statement. *Omnicare, Inc. v. Laborers Dist. Council Constr. Indus. Pension Fund*, 575 U.S. 175, 188 (2015). When a speaker omits facts that "conflict with what a reasonable investor would take from the statement itself," the statement may be misleading. *Id.* at 189.

The second question is whether the misleading statement is material. Answering that question, too, requires a totality-of-the-circumstances inquiry. In the securities context, material facts are those that investors likely would consider important to their securities-buying decisions. "[T]o fulfill the materiality requirement 'there must be a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the "total mix" of information made available.'" *Basic*, 485 U.S. at 231-32 (quoting *TSC Indus.*, 426 U.S. at 449).

2. SEC rules require companies to disclose "Risk Factors" that make investments in the companies' securities speculative or risky. 17 C.F.R. § 229.503(c) (2017). In February 2018, the SEC published interpretive guidance meant to assist public companies preparing disclosures about cybersecurity risks and incidents. *See* Interpretation, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8169 (Feb. 26, 2018) ("*Cybersecurity Disclosures*"). The guidance details what factors companies should consider when deciding whether a cybersecurity incident or risk is material

under federal securities laws. *See id.* at 8168-69. Agency interpretations like this can provide "the judgments about the way the real world works" that "are precisely the kind that agencies are better equipped to make than are courts." *Pension Benefit Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 651 (1990). This Court therefore has observed that "the SEC's view of the proper balance between the need to insure adequate disclosure and the need to avoid the adverse consequences of setting too low a threshold for civil liability is entitled to consideration." *TSC Indus.*, 426 U.S. at 449 n.10.

The SEC's interpretive guidance is context-specific: "The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude" as well as "the range of harm that such incidents could cause." *Cybersecurity Disclosures*, 83 Fed. Reg. at 8169. "As part of a materiality analysis, a company should consider the indicated probability that an event will occur and the anticipated magnitude of the event in light of the totality of company activity" and "the nature of the company's business." *Id.* at 8169 nn.33 & 34. Most relevant here, "[i]n meeting their disclosure obligations, *companies may need to disclose previous or ongoing cybersecurity incidents or other past events* in order to place discussions of these risks in the appropriate context." *Id.* at 8169-70 (emphasis added).

B. The Ninth Circuit Correctly Determined Google's Risk Disclosures Were Materially Misleading Under The Circumstances

The Ninth Circuit rightly concluded that Google's quarterly report risk disclosures were materially misleading. The complaint alleges that Google had undisclosed information of an important and ongoing

risk to the data security of its hundreds of millions of Google+ users. Google's failure to disclose that information made its generic risk statements misleading and significantly altered the "total mix" of information available to investors.

1. In context, Google's risk disclosures in its April and July 2018 quarterly reports were misleading. Like any other statement by a public company, risk disclosures may be misleading if they omit information that "conflict[s] with what a reasonable investor would take from" the disclosures. *Omnicare*, 575 U.S. at 189. The complaint alleges that Google had discovered widespread security vulnerabilities that it could not contain and that made data leaks inevitable. The company deliberated about whether to disclose these issues to investors. To avoid regulatory scrutiny in the wake of the Cambridge Analytica scandal, Google chose to cover up its issues instead. The cover-up extended to the company's quarterly reports, which said there had been "no material changes" to the company's risk factors. *See supra* p. 7. That statement left reasonable investors with the false impression that Google's data-security risk profile had remained largely the same when it had dramatically changed. Under these circumstances, the Ninth Circuit correctly concluded that "the omission of any mention of the Three-Year Bug or the other security vulnerabilities made the statements in each Form 10-Q materially misleading to a reasonable investor." App. 22a-23a.

Google had characterized the complaint as being about a failure to disclose an isolated, past event, arguing that this omission could not make its statement of future risks misleading. The Ninth Circuit correctly rejected the company's description of both

the facts and the law. In April 2018, the Three-Year Bug was not a "past" event; Google still was dealing with the fallout. The complaint alleges Google "could only identify two weeks' worth of users whose private profile information had been exposed," ER35 (¶ 37); that the company had "insufficient records to determine whether a breach occurred," ER41(¶ 59); and that the public "may never know the full extent of the damage caused by the failure to provide adequate controls and protection to users," ER42(¶ 59). The Three-Year Bug exposed significant problems with Google's ability to find and fix security issues. The company could not just patch the bug – it had to determine how the bug had remained undetected for three years. "Given that Google's business model is based on trust, the material implications of a bug that improperly exposed user data for three years were not eliminated merely by plugging the hole in Google+'s security." App. 26a.

The Three-Year Bug also was not an isolated event. The complaint alleges it was "just the tip of the iceberg." ER46 (¶ 73). The Privacy Bug Memo "highlighted additional security vulnerabilities that were so significant that they allegedly led to Google's decision to shut down the Google+ consumer platform." App. 26a. And these vulnerabilities were not hypothetical: the complaint alleges that the memo conveyed that "additional data exposures" were "virtually inevitable." ER36 (¶ 38). This prediction proved accurate. Later the same year, the company suffered another data exposure involving more than 50 million Google+ users. ER43 (¶ 64). The Ninth Circuit rightly rejected Google's argument that its failure to disclose an isolated, past risk could not mislead reasonable investors because the complaint alleges undisclosed present, pervasive issues.

Setting aside those factual issues, Google's argument lacks legal merit. In its interpretive guidance, the SEC discussed a hypothetical situation much like Google's, involving a company that "previously experienced a material cybersecurity incident involving denial-of-service." *Cybersecurity Disclosures*, 83 Fed. Reg. at 8170. For such a company, "it likely would not be sufficient . . . to disclose that there is a risk that a denial-of-service incident *may* occur." *Id.* (emphasis added). Instead, "to effectively communicate cybersecurity risks to investors," "the company may need to discuss the occurrence of that cybersecurity incident and its consequences." *Id.* The longstanding precedent the Ninth Circuit applied tracked that guidance: "Risk disclosures that 'speak[] entirely of as-yet-unrealized risks and contingencies' and do not 'alert[] the reader that some of these risks may already have come to fruition' can mislead reasonable investors." App. 24a (quoting *Berson v. Applied Signal Tech., Inc.*, 527 F.3d 982, 985-87 (9th Cir. 2008)) (alterations below). Under that settled law, the court correctly held that "the complaint plausibly alleges that [Google's] warnings in each [quarterly report] of risks that 'could' or 'may' occur is misleading to a reasonable investor when [Google] knew that those risks had materialized." App. 25a.

2. Google's misleading omissions were material. The "materiality requirement is satisfied when there is 'a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the "total mix" of information made available.'" *Matrixx*, 563 U.S. at 38 (quoting *Basic*, 485 U.S. at 231-32).

Cybersecurity incidents are often relevant to investor decisionmaking because they involve many

potentially substantial costs: As the Ninth Circuit noted, these incidents can lead to "'harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions.'" App. 24a (quoting *Cybersecurity Disclosures*, 83 Fed. Reg. at 8168-69). Data-privacy issues are more relevant still to a company like Google, which operates in an industry based on security. *See Cybersecurity Disclosures*, 83 Fed. Reg. at 8169 n.33 (materiality of cybersecurity incidents "may depend on the nature of the company's business"). Google's business model requires its users to trust the company with their data, which Google monetizes by selling targeted ads. In the words of the company's former Executive Chairman, a breach of user trust, like a significant data leak, "would be devastating." ER27 (¶ 20). The Privacy Bug Memo made clear that a major breach of user trust was inevitable. It "highlighted additional security vulnerabilities that were so significant that they allegedly led to Google's decision to shut down the Google+ consumer platform." App. 26a. Public disclosure of Google's serious failings could have wide-ranging effects: "users and customers may curtail or stop using our products and services, and we may incur significant legal and financial exposure." ER30 (¶ 27(b)) (emphasis omitted). The importance of those risks makes it more than plausible that information about the many extant security issues Google had uncovered would have been substantially likely to alter the total mix of information available to Google's investors.

The reaction to the *Wall Street Journal*'s article confirms that the Privacy Bug – and Google's efforts to conceal it – was material. Right after publication,

the result was "a swift stock price decline, legislative scrutiny, and public reaction, all of which support the allegation that the Privacy Bug was material even absent a release of sensitive information or revenue decline." App. 27a.

The Ninth Circuit correctly applied this Court's contextual rule to the allegations in the complaint, finding Google's omissions were materially misleading. Google's disagreement with that factbound conclusion does not merit this Court's review.

C. Petitioners' Bright-Line Rule Finds No Support In This Court's Precedents

Like the defendants in *Basic*, *Matrixx*, and *Omnicare*, Google "urges [this Court] to adopt a bright-line rule," *Matrixx*, 563 U.S. at 39, that a company's failure to disclose a past event in its risk disclosures never can be materially misleading. Pet. 24. Because this case does not involve a failure to disclose an isolated, past risk, it presents no opportunity to adopt such a rule. *See supra* pp. 16-17. And in any event, Google's proposed rule does not fit the totality-of-the-circumstances inquiry this Court uses to determine whether a statement or omission is misleading and material.

1. Whenever a company speaks, it must disclose the facts necessary to make its statements, "'in the light of the circumstances under which they were made, not misleading.'" *Matrixx*, 563 U.S. at 37 (quoting 17 C.F.R. § 240.10b-5(b)). Google argues that a risk disclosure "that discloses only future potential harms is not misleading to a reasonable investor." Pet. 24. The company's cornerstone argument is that past events can never be a "risk," which it defines as "[t]he possibility of suffering harm or loss"; "the chance of injury, damage, or loss"; or "the possibility

of loss." *Id.* (citations omitted; brackets in original). But the issues identified in the Privacy Bug Memo were present "risks" under any definition of the term. Under the circumstances, those ongoing issues involved "the possibility of loss" even after Google programmers fixed some of Google+'s faulty code. *See supra* pp. 16-17.[4]

Google's account of what a reasonable investor would find misleading is blind to context. "On [the company's] view, no reasonable person, in any context, can understand" a risk disclosure "to convey anything more than" future risks. *Omnicare*, 575 U.S. at 187. In *Omnicare*, the defendant similarly argued that "a pure statement of opinion" cannot "convey anything more than the speaker's own mindset." *Id.* But that categorical argument was not categorically true: "[I]f the real facts are otherwise, but not provided, the opinion statement will mislead its audience." *Id.* at 188. For example, "an unadorned statement of opinion about legal compliance" – "'We believe our

---

[4] At times, Google's petition suggests that *no* risk disclosures – not just those that omit material past events – ever can be misleading to a reasonable investor. Pet. 24; *see also* WLF Br. 2. The company tries to soften this hard rule by stating that "a company's statement that 'no current security concerns exist' or that it had 'never' experienced a security issue – when in fact a security issue was ongoing or had occurred in the past – might be subject to liability under Section 10(b), depending on the circumstances." Pet. 25-26. But this carveout is illusory because no company would make such a statement. Risk disclosures are about "the most significant factors that make the offering speculative or risky," 17 C.F.R. § 229.503(c) (2017), not nonexistent risks, as in Google's example. And all companies face some degree of cybersecurity concerns, as both Google and *amici* state. *See* Pet. 31; Chamber Br. 5 ("Cyberattacks, data breaches, and security bugs are an omnipresent risk for companies.").

conduct is lawful'" – "could be misleadingly incomplete" if "the issuer ma[de] that statement without having consulted a lawyer." *Id.*

So too here. Google offered general assurances of unchanged risks in the face of specific known and significantly greater risks. In a case some years ago, Judge Pollack analogized that approach to "someone who warns his hiking companion to walk slowly because there might be a ditch ahead when he knows with near certainty that the Grand Canyon lies one foot away." *In re Prudential Sec. Inc. Ltd. P'ships Litig.*, 930 F. Supp. 68, 72 (S.D.N.Y. 1996). Like the hiker, Google failed to disclose its own Grand Canyon – the Three-Year Bug and the issues in the Privacy Bug Memo. This made its boilerplate risk disclosures misleading "in the light of the circumstances under which they were made."

2. Nor can Google's proposed bright-line rule be squared with this Court's precedent on materiality. This Court unanimously rejected similar rules in *Basic* and *Matrixx*. In each case, the Court recognized that such a "categorical rule would 'artificially exclud[e]' information that 'would otherwise be considered significant to the trading decision of a reasonable investor.'" *Matrixx*, 563 U.S. at 40 (quoting *Basic*, 485 U.S. at 236) (alteration in *Matrixx*).

3. Google offers "no valid justification for artificially excluding [past-event disclosures] from the definition of materiality." *Basic*, 485 U.S. at 236. The company argues that requiring companies to disclose material realized risks in their SEC filings will lead to over-disclosure, "drown[ing] out the forward-looking information investors and potential investors actually need." Pet. 28. This echoes the defendant's argument in *Matrixx* that failure to adopt its rule would lead

companies to disclose "'an avalanche of trivial information.'" *Matrixx*, 563 U.S. at 38 (quoting *Basic*, 485 U.S. at 231). This Court rejected that argument in *Matrixx*, and it is no more persuasive here.

Applying *Basic*'s "total mix" standard does not mean that companies must disclose *all* past data-security issues. As this Court observed in *Matrixx*, "[t]he question remains whether a *reasonable* investor would have viewed the nondisclosed information 'as having *significantly* altered the "total mix" of information made available.'" *Id.* at 44 (quoting *Basic*, 485 U.S. at 231-32) (emphases in *Matrixx*). That has been the rule for decades, and it has not led to the over-disclosure of which Google warns.

4. If Google's predictions of over-disclosure had merit, they would have come true long ago. Companies operating in the Ninth Circuit have been on notice for at least 14 years that their forward-looking statements in SEC filings may have to include certain risks that "already have come to fruition." *Berson*, 527 F.3d at 986.

In *Berson*, a government contractor faced securities suits when its revenue dropped 25% following the cancellation of several contracts. The contracts at issue were subject to "stop-work" orders, which stop payment to the company and often signal that the contracts will be cancelled. Yet the contractor included revenue from those contracts as part of the "backlog" of work the company had contracted to do, but had not yet performed. In SEC filings, the company warned that "future changes in delivery schedules and cancellations of orders" might mean sales for the year would not match the full backlog value. *Id.* The court found that disclosure misleading. It spoke "entirely of as-yet-unrealized risks" – "[n]othing alerts the reader

that some of these risks may already have come to fruition, and that what the company refers to as backlog includes work that is substantially delayed and at serious risk of being cancelled altogether." *Id.* The Ninth Circuit's analysis here tracked *Berson*. App. 24a. If *Berson* did not lead to over-disclosure, neither will the decision below.

Similarly, companies operating nationwide have been on notice for at least 11 years that their risk disclosures may need to detail past cybersecurity incidents. In 2011, the SEC published a guidance document on cybersecurity risks, which it then updated in 2018. *See supra* pp. 14-15. In the 2011 document, the Commission offered the hypothetical of a company that "experienced a material cyber attack in which malware was embedded in its systems and customer data was compromised." Div. of Corp. Fin., CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011), http://sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. There, "it likely would not be sufficient for the registrant to disclose that there is a risk that such an attack may occur." *Id.* "Instead, as part of a broader discussion of malware or other similar attacks that pose a particular risk, the registrant may need to discuss the occurrence of the specific attack and its known and potential costs and other consequences." *Id.* That contextual rule is the same one that the SEC reaffirmed in 2018 and that the Ninth Circuit applied below.

II. THERE IS NO CIRCUIT CONFLICT

A. The Circuits Agree That Whether Risk Disclosures Are Materially False Depends On Context

In every other circuit to have considered the issue, a risk disclosure that fails to mention that a risk has

taken place *may* be materially misleading depending on the context.

That is the rule in the First Circuit, which has observed that a company might be liable for vague and hypothetical risk disclosures if it knew the warned-of risk was actually occurring. *See Karth v. Keryx Biopharms., Inc.*, 6 F.4th 123, 138 (1st Cir. 2021); *see also Hill v. Gozani*, 638 F.3d 40, 60 (1st Cir. 2011) (affirming dismissal but noting that "[a] statement that discloses a level of risk may be so understated as to be misleading"). In *Karth*, the defendant had warned it might suffer interruptions in its supply chain. That statement, when made, was true: the alleged facts "d[id] not indicate that a supply interruption was happening or was even close to a 'near certainty.'" 6 F.4th at 138. The plaintiff therefore had not plausibly alleged materiality.

The Third Circuit has taken the same tack. That court "agree[d] that a company may be liable under Section 10b for misleading investors when it describes as hypothetical a risk that has already come to fruition." *Williams v. Globus Med., Inc.*, 869 F.3d 235, 242 (3d Cir. 2017). *Williams* "[wa]s not such a case." *Id.* There, the defendant decided to end its relationship with a distributor. The Third Circuit held that the defendant did not have to disclose that decision when it had not yet impacted sales and there was no alleged "inevitable" drop forthcoming. *Id.* at 243.

Similarly, the Sixth Circuit has recognized that "there may be circumstances under which a risk disclosure might support Section 10(b) liability." *Bondali v. Yum! Brands, Inc.*, 620 F. App'x 483, 491 (6th Cir. 2015). *Bondali* did not involve such a circumstance. There, Kentucky Fried Chicken failed to inform investors that "eight batches of chicken

test[ed] positive for drug and antibiotic residues." *Id.* That was "hardly a companywide food safety epidemic, and the plaintiffs allege[d] no facts to suggest otherwise." *Id.* The company's generic statements that food-safety issues "have occurred in the past, and could occur in the future," were therefore not materially misleading. *Id.* at 490.

The D.C. Circuit applied the same rule in *In re Harman International Industries, Inc. Securities Litigation*, 791 F.3d 90 (D.C. Cir. 2015), *cert. denied*, 577 U.S. 1139 (2016). The defendant – a manufacturer of car entertainment and guidance systems – touted its considerable inventory of devices but warned generally that its sales depended on its ability to develop new products in a competitive market. *Id.* at 103-04. The company did not disclose to investors that much of its inventory had been rendered obsolete by new technology, forcing the company to cut its prices and reducing its sales revenue. The D.C. Circuit said the company's general warnings about product obsolescence could be misleading, emphasizing that "there is an important difference between warning that something '*might*' occur and that something '*actually* had' occurred." *Id.* at 103.[5]

---

[5] The SEC adopted this theory in a civil case against Facebook arising out of the Cambridge Analytica scandal. The core of the SEC's case was that "Facebook's public disclosures presented the risk of misuse of user data as merely hypothetical when Facebook knew that a third-party developer had actually misused Facebook user data." Press Release, SEC, *Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data* (July 24, 2019), https://www.sec.gov/news/press-release/2019-140. The SEC warned public companies not to "continu[e] to describe a risk as hypothetical when it has in fact happened." *Id.* Facebook settled for $100 million. *Id.*

Whether a risk disclosure must include a past event depends on whether it still would be relevant to a reasonable investor. In every circuit, when a company's decision to omit a past event from its risk disclosures makes those disclosures misleading and significantly alters the "total mix" of information made available to investors, that decision may lead to liability. *Basic*, 485 U.S. at 231-32.

B. Google's Purported Circuit Split Is Illusory

Petitioners claim the Fourth and Sixth Circuits have held that companies never need disclose past events in their risk disclosures. Pet. 16. But that contention does not withstand scrutiny.

The Sixth Circuit follows no such rule. The panel in *Bondali* said that "cautionary statements are not actionable to the extent plaintiffs contend defendants should have disclosed risk factors 'are' affecting financial results rather than 'may' affect financial results." 620 F. App'x at 491 (internal quotation marks omitted). But the court elsewhere recognized that there "may be circumstances under which [such] a risk disclosure might support Section 10(b) liability." *Id.* In any event, the first statement was unnecessary to the result: the court would have affirmed regardless because "the plaintiffs ha[d] not alleged facts showing any investment risk had already materialized." *Id.* And the Sixth Circuit has not adopted *Bondali*'s dictum as the law of the circuit. The opinion is unpublished, and "[u]npublished decisions in the Sixth Circuit are, of course, not binding precedent on subsequent panels." *Crump v. Lafler*, 657 F.3d 393, 405 (6th Cir. 2011). District courts within the Sixth Circuit thus have disregarded the decision, holding that *Bondali* does not foreclose liability for risk disclosures. *See*, *e.g.*, *Weiner v. Tivity Health, Inc.*, 365

F. Supp. 3d 900, 909-10 (M.D. Tenn. 2019) ("*Bondali* is unpublished and therefore not 'binding precedent' or 'binding authority'").

The Fourth Circuit has said even less in Google's favor. The company relies on *Dice v. Channeladvisor Corp.*, 671 F. App'x 111 (4th Cir. 2016) (per curiam). Pet. 17. But *Dice* is an unpublished summary affirmance with no substantive reasoning.

Finally, Google cites three district court opinions it claims support its approach. But in none of those cases was Google's categorical rule necessary to the result. In *In re ChannelAdvisor Corp. Securities Litigation*, which the Fourth Circuit affirmed in *Dice*, the defendant had "laid all its cards on the table through its various statements and disclosures. No material information was omitted." 2016 WL 1381772, at *4 (E.D.N.C. Apr. 6, 2016). In *In re Marriott International, Inc., Customer Data Security Breach Litigation*, the defendant experienced a serious data breach, and its risk disclosures after the breach stated that it had experienced cyber-attacks. 2021 WL 2407518, at *24 (D. Md. June 11, 2021), *appeal pending*, No. 21-1802 (4th Cir.). And in *Indiana Public Retirement System v. Pluralsight, Inc.*, the court recognized that "'a risk disclosure might support Section 10(b) liability.'" 2021 WL 1222290, at *14 (D. Utah Mar. 31, 2021) (quoting *Bondali*, 620 F. App'x at 491), *appeal pending*, No. 21-4058 (10th Cir.). The court did not adopt the bright-line rule Google urges here. Instead, it found that, under the specific circumstances presented there, "[a] reasonable investor would be unlikely to read Statement 12's generic language about Pluralsight expanding its sales efforts and investing in sales and marketing and be misled into thinking that Pluralsight either was or was not behind in its sales force ramping capacity." *Id.* In

fact, "it [wa]s not apparent that the risk entailed by Pluralsight being behind in its sales ramp capacity plan had manifested at the time that the company filed its 2018 Form 10-K." *Id*. at *15.

There is no reason to depart from this Court's general practice of "permitting several courts of appeals to explore" an issue and "waiting for a conflict to develop" before granting review. *United States v. Mendoza*, 464 U.S. 154, 160 (1984).

III. THIS CASE PRESENTS A POOR VEHICLE FOR ADDRESSING THE QUESTION PRESENTED

Even if the decision below were wrong and the circuits were split, certiorari should be denied because this case is a poor vehicle. First, the case is highly factbound. The Ninth Circuit focused on a unique set of allegations that combined to make Google's disclosures materially misleading. The company uncovered not just the Three-Year Bug – the scope and impact of which the company could not determine – but also gaps in its security that made future bugs unavoidable. Those future bugs were so dangerous that Google decided to shut down Google+, which was then one of the largest social media networks in the world. And even though Google's business model was founded on user trust, the company chose to conceal those risks to avoid the unprecedented public and legislative attention then being paid to data security. Given *all* these factors, "the complaint plausibly alleges that the omission of any mention of the Three-Year Bug or the other security vulnerabilities made the statements in each [quarterly report] materially misleading to a reasonable investor and significantly altered the total mix of information available to investors." App. 22a-23a.

Second, this Court's review will not fully resolve the case. No matter the answer to the question presented, Rhode Island Employees' Retirement System has surviving claims under Rule 10b-5(a) and (c), and Section 20(a), which Google never has moved to dismiss and which the petition leaves undisturbed. App. 37a. If there is sufficient evidence to go to trial, this Court will have another opportunity to determine the appropriate standard for a company's risk disclosures and to resolve all these claims together. For now, this Court need not intervene just to save a trillion-dollar company the cost of discovery into its misconduct.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted,

JASON A. FORGE
ROBBINS GELLER RUDMAN & DOWD LLP
655 West Broadway
Suite 1900
San Diego, CA 92101
(619) 231-1058

DAVID C. FREDERICK
Counsel of Record
DEREK C. REINBOLD
KELLOGG, HANSEN, TODD, FIGEL & FREDERICK, P.L.L.C.
1615 M Street, N.W.
Suite 400
Washington, D.C. 20036
(202) 326-7900
(dfrederick@kellogghansen.com)

February 2, 2022