

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-Q

(Mark One)

- ☒ **QUARTERLY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the quarterly period ended April 30, 2026
or
☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the transition period from _____ to _____
Commission File Number: 001-42028

RUBRIK, INC.

(Exact name of registrant as specified in its charter)

Delaware
(State or other jurisdiction of
incorporation or organization)

46-4560494
(I.R.S. Employer
Identification No.)

3495 Deer Creek Road, Palo Alto, California 94304
(Address of principal executive offices and zip code)

(844) 478-2745
(Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Class A Common Stock, \$0.000025 par value	RBRK	New York Stock Exchange

Indicate by checkmark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15 (d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports) and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

- | | | | |
|-------------------------|-------------------------------------|---------------------------|--------------------------|
| Large accelerated filer | ☒ | Accelerated filer | ☐ |
| Non-accelerated filer | ☐ | Smaller reporting company | ☐ |
| | | Emerging growth company | ☐ |

If an emerging growth company, indicate by check mark if the Registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

As of May 31, 2026, Rubrik Inc. had 160,956,763 shares of Class A common stock outstanding, and 44,871,803 shares of Class B common stock outstanding.

Rubrik, Inc.
FORM 10-Q
For the Fiscal Quarter Ended April 30, 2026
TABLE OF CONTENTS

PART I. FINANCIAL INFORMATION

Item 1.	Financial Statements (unaudited)	5
	Condensed Consolidated Balance Sheets	5
	Condensed Consolidated Statements of Operations	6
	Condensed Consolidated Statements of Comprehensive Loss	7
	Condensed Consolidated Statements of Stockholders' Deficit	8
	Condensed Consolidated Statements of Cash Flows	9
	Notes to Condensed Consolidated Financial Statements	10
Item 2.	Management's Discussion and Analysis of Financial Condition and Results of Operations	22
Item 3.	Quantitative and Qualitative Disclosures About Market Risk	36
Item 4.	Controls and Procedures	36

PART II. OTHER INFORMATION

Item 1.	Legal Proceedings	38
Item 1A.	Risk Factors	38
Item 2.	Unregistered Sales of Equity Securities and Use of Proceeds	77
Item 3.	Defaults Upon Senior Securities	77
Item 4.	Mine Safety Disclosures	77
Item 5.	Other Information	77
Item 6.	Exhibits	78
	Signatures	79

SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

This Quarterly Report on Form 10-Q contains forward-looking statements about us and our industry that involve substantial risks and uncertainties. All statements other than statements of historical facts contained in this Quarterly Report on Form 10-Q, including statements regarding our future financial condition or results of operations, business strategy and plans, and objectives of management for future operations are forward-looking statements. In some cases, you can identify forward-looking statements because they contain words such as “anticipate,” “believe,” “continue,” “could,” “estimate,” “expect,” “intend,” “may,” “plan,” “potential,” “predict,” “project,” “should,” “target,” “toward,” “will,” “would,” or the negative of these words or other similar terms or expressions. These forward-looking statements include, but are not limited to, statements concerning the following:

- our expectations regarding our revenue, cost of revenue, gross profit or gross margin, operating expenses, and other results of operations, including our key metrics;
- the growth rate of the market in which we compete;
- our business plan and our ability to effectively manage our growth and associated investments;
- anticipated trends, growth rates, and challenges in our business and in the markets in which we operate;
- our ability to achieve or sustain our profitability;
- future investments in our business, our anticipated capital expenditures, and our estimates regarding our capital requirements;
- the costs and success of our marketing efforts and our ability to promote our brand;
- our ability to increase sales of our products;
- our ability to acquire new customers and successfully retain and expand platform usage with existing customers;
- our ability and expectations to continue to innovate and enhance our platform;
- our ability to operate our business under evolving macroeconomic conditions, such as high inflation, bank failures and related uncertainties, or recessionary or uncertain environments, and supply chain disruptions, including global semiconductor or hardware component shortages;
- our ability to compete effectively with existing competitors and new market entrants;
- our ability to introduce new products on top of our platform; and
- our expectations regarding our convertible senior notes due June 2030, including the expected use of proceeds we received and our ability to meet the requirements of the notes.

We caution you that the foregoing list may not contain all of the forward-looking statements made in this Quarterly Report on Form 10-Q.

You should not rely on forward-looking statements as predictions of future events. We have based the forward-looking statements contained in this Quarterly Report on Form 10-Q primarily on our current expectations and projections about future events and trends that we believe may affect our business, financial condition, and results of operations. The outcome of the events described in these forward-looking statements is subject to risks, uncertainties, and other factors described in the section titled “Risk Factors” and elsewhere in this Quarterly Report on Form 10-Q. Moreover, we operate in a very competitive and rapidly changing environment. New risks and uncertainties emerge from time to time, and it is not possible for us to predict all risks and uncertainties that could have an impact on the forward-looking statements contained in this Quarterly Report on Form 10-Q. The results, events, and circumstances reflected in the forward-looking statements may not be achieved or occur, and actual results, events, or circumstances could differ materially from those described in the forward-looking statements.

In addition, statements that “we believe” and similar statements reflect our beliefs and opinions on the relevant subject. These statements are based on information available to us as of the date of this Quarterly Report on Form 10-Q. While we believe such information provides a reasonable basis for these statements, such information may be limited or incomplete. Our statements should not be read to indicate that we have conducted an exhaustive inquiry into, or review of, all relevant information. These statements are inherently uncertain, and investors are cautioned not to unduly rely on these statements.

The forward-looking statements made in this Quarterly Report on Form 10-Q relate only to events as of the date on which the statements are made. We undertake no obligation to update any forward-looking statements made in this Quarterly Report on Form 10-Q to reflect events or circumstances after the date of this Quarterly Report on Form 10-Q or to reflect new information, actual results, revised expectations, or the occurrence of unanticipated events, except as required by law. We may not actually achieve the plans, intentions, or expectations disclosed in our forward-looking statements, and you should not place undue reliance on our forward-looking statements. Our forward-looking statements do not reflect the potential impact of any future acquisitions, mergers, dispositions, joint ventures, or investments.

Risk Factors Summary

Below is a summary of the principal factors that make an investment in our Class A common stock speculative or risky:

- Our recent rapid growth may not be indicative of our future growth. Our rapid growth also makes it difficult to evaluate our future prospects.
- If the market for data security and AI solutions does not grow, our ability to grow our business and our results of operations may be adversely affected.
- We have a limited operating history, particularly with respect to our offerings of Rubrik Security Cloud and Rubrik Agent Cloud, which makes it difficult to forecast our future results of operations.
- If we are unable to attract new customers, our future results of operations could be harmed.
- We have a history of operating losses and may not achieve or sustain profitability in the future.
- If our customers do not renew their subscriptions for our platform and products or expand their subscriptions to increase the amount of data secured, secure new applications, or include new features or capabilities, our results of operations could be harmed.
- If our solutions fail or do not perform as intended or are perceived to have defects, errors, or vulnerabilities, our brand and reputation will be harmed, which would adversely affect our business and results of operations.
- Our information technology systems or data, or those of third parties with whom we work, have in the past been, and may in the future be, compromised, which may cause us to experience significant adverse consequences, including but not limited to regulatory investigations or actions, litigation, fines and penalties, disruptions of our business operations, reputational harm, loss of revenue or profits, loss of customers or sales, and other adverse consequences. As a data security company, we have been and may in the future be specifically targeted by various threat actors who try to compromise our information technology systems or data.
- The limited number of contract manufacturers and original equipment manufacturers that produce commodity servers that are compatible with our solutions are susceptible to supply chain disruptions and have recently experienced shortages of key components for their servers, which may adversely affect our ability to accurately forecast demand for these commodity servers or successfully manage the relationship with such manufacturers, and could negatively impact demand for our offerings, and adversely affect our business and financial results.
- Our use of generative, agentic and other artificial intelligence tools may pose risks to business and operations, including our proprietary software and systems, and may subject us to legal liability.
- We rely upon third-party cloud providers to host our solutions, and any disruption of, or interference with, our use of third-party cloud products would adversely affect our business, financial condition, and results of operations.
- We may not be able to successfully manage our growth, and if we are not able to grow efficiently, our business, financial condition, and results of operations could be harmed.
- The markets in which we participate are competitive, and if we do not compete effectively, our business, financial condition, and results of operations could be harmed.
- Our estimates of market opportunity, forecasts of market growth, and potential return on investment may prove to be inaccurate, and even if the market in which we compete achieves the forecasted growth, our business could fail to grow at similar rates, if at all.
- The dual class structure of our common stock has the effect of concentrating voting control with the holders of our Class B common stock, including our executive officers, employees, and directors and their affiliates, and limiting your ability to influence corporate matters, which could adversely affect the trading price of our Class A common stock.

PART I. FINANCIAL INFORMATION

Item 1. Financial Statements (unaudited)

Rubrik, Inc. **CONDENSED CONSOLIDATED BALANCE SHEETS** (in thousands, except share and par value amounts) (unaudited)

	April 30, 2026	January 31, 2026
Assets		
Current assets		
Cash and cash equivalents	\$ 429,397	\$ 380,196
Short-term investments	1,319,717	1,295,579
Accounts receivable, net of allowances of \$546 and \$299	199,344	256,773
Deferred commissions	109,910	110,651
Prepaid expenses and other current assets	165,368	180,365
Total current assets	2,223,736	2,223,564
Property and equipment, net	86,504	83,830
Deferred commissions, noncurrent	155,621	157,592
Goodwill	199,606	199,606
Other assets, noncurrent	102,780	101,944
Total assets	\$ 2,768,247	\$ 2,766,536
Liabilities and stockholders' deficit		
Current liabilities		
Accounts payable	\$ 14,161	\$ 15,329
Accrued expenses and other current liabilities	143,910	229,976
Deferred revenue	1,121,975	1,068,754
Total current liabilities	1,280,046	1,314,059
Deferred revenue, noncurrent	766,401	776,547
Other liabilities, noncurrent	71,334	64,771
Convertible senior notes, net	1,131,791	1,130,721
Total liabilities	3,249,572	3,286,098
Commitments and contingencies (Note 8)		
Stockholders' deficit		
Preferred stock, \$0.000025 par value – 20,000,000 shares authorized as of April 30, 2026 and January 31, 2026; zero shares issued and outstanding as of April 30, 2026 and January 31, 2026	—	—
Class A common stock, \$0.000025 par value – 1,070,000,000 shares authorized as of April 30, 2026 and January 31, 2026; 160,945,763 and 157,370,648 shares issued and outstanding as of April 30, 2026 and January 31, 2026, respectively	4	4
Class B common stock, \$0.000025 par value – 210,000,000 shares authorized as of April 30, 2026 and January 31, 2026; 44,871,803 and 44,871,492 shares issued and outstanding as of April 30, 2026 and January 31, 2026, respectively	1	1
Additional paid-in capital	2,755,906	2,662,861
Accumulated other comprehensive (loss) income	(9,222)	3,733
Accumulated deficit	(3,228,014)	(3,186,161)
Total stockholders' deficit	(481,325)	(519,562)
Total liabilities and stockholders' deficit	\$ 2,768,247	\$ 2,766,536

The accompanying notes are an integral part of these unaudited condensed consolidated financial statements.

Rubrik, Inc.
CONDENSED CONSOLIDATED STATEMENTS OF OPERATIONS
(in thousands, except per share amounts)
(unaudited)

	Three Months Ended April 30,	
	2026	2025
Revenue		
Subscription	\$ 374,153	\$ 265,661
Other	12,915	12,820
Total revenue	387,068	278,481
Cost of revenue		
Subscription	66,723	51,912
Other	8,562	8,571
Total cost of revenue	75,285	60,483
Gross profit	311,783	217,998
Operating expenses		
Research and development	114,341	81,815
Sales and marketing	193,098	169,993
General and administrative	56,978	59,281
Total operating expenses	364,417	311,089
Loss from operations	(52,634)	(93,091)
Interest income	15,898	7,696
Interest expense	(1,070)	(9,813)
Other income (expense), net	590	(5,622)
Loss before income taxes	(37,216)	(100,830)
Income tax expense	4,637	1,274
Net loss	\$ (41,853)	\$ (102,104)
Net loss per share, basic and diluted	\$ (0.21)	\$ (0.53)
Weighted-average shares used in computing net loss per share, basic and diluted	203,668	191,625

The accompanying notes are an integral part of these unaudited condensed consolidated financial statements.

Rubrik, Inc.
CONDENSED CONSOLIDATED STATEMENTS OF COMPREHENSIVE LOSS
(in thousands)
(unaudited)

	Three Months Ended April 30,	
	2026	2025
Net loss	\$ (41,853)	\$ (102,104)
Foreign currency translation adjustment, net of tax	(9,019)	8,751
Unrealized (loss) gain on available-for-sale securities, net of tax	(3,936)	41
Total other comprehensive (loss) income, net of tax	(12,955)	8,792
Comprehensive loss	<u>\$ (54,808)</u>	<u>\$ (93,312)</u>

The accompanying notes are an integral part of these unaudited condensed consolidated financial statements.

Rubrik, Inc.
CONDENSED CONSOLIDATED STATEMENTS OF STOCKHOLDERS' DEFICIT
(in thousands, except share amounts)
(unaudited)

Three Months Ended April 30, 2026						
	Common stock		Additional paid-in capital	Accumulated other comprehensive income (loss)	Accumulated deficit	Total stockholders' deficit
	Shares	Amount				
Balances as of January 31, 2026	202,242,140	\$ 5	\$ 2,662,861	\$ 3,733	\$ (3,186,161)	\$ (519,562)
Issuance of common stock upon exercise of stock options	152,660	—	643	—	—	643
Issuance of common stock upon settlement of restricted stock units	2,881,121	—	—	—	—	—
Issuance of common stock under employee stock purchase plan	541,645	—	16,559	—	—	16,559
Stock-based compensation	—	—	75,843	—	—	75,843
Other comprehensive loss	—	—	—	(12,955)	—	(12,955)
Net loss	—	—	—	—	(41,853)	(41,853)
Balances as of April 30, 2026	<u>205,817,566</u>	<u>\$ 5</u>	<u>\$ 2,755,906</u>	<u>\$ (9,222)</u>	<u>\$ (3,228,014)</u>	<u>\$ (481,325)</u>
Three Months Ended April 30, 2025						
	Common stock		Additional paid-in capital	Accumulated other comprehensive (loss) income	Accumulated deficit	Total stockholders' deficit
	Shares	Amount				
Balances as of January 31, 2025	189,766,790	\$ 5	\$ 2,291,829	\$ (8,235)	\$ (2,837,333)	\$ (553,734)
Issuance of common stock upon exercise of stock options	197,534	—	1,875	—	—	1,875
Issuance of common stock upon settlement of restricted stock units	2,923,098	—	—	—	—	—
Issuance of common stock under employee stock purchase plan	494,926	—	13,492	—	—	13,492
Stock-based compensation	—	—	75,149	—	—	75,149
Other comprehensive income	—	—	—	8,792	—	8,792
Net loss	—	—	—	—	(102,104)	(102,104)
Balances as of April 30, 2025	<u>193,382,348</u>	<u>\$ 5</u>	<u>\$ 2,382,345</u>	<u>\$ 557</u>	<u>\$ (2,939,437)</u>	<u>\$ (556,530)</u>

The accompanying notes are an integral part of these unaudited condensed consolidated financial statements.

Rubrik, Inc.
CONDENSED CONSOLIDATED STATEMENTS OF CASH FLOWS
(in thousands)
(unaudited)

	Three Months Ended April 30,	
	2026	2025
Cash flows from operating activities:		
Net loss	\$ (41,853)	\$ (102,104)
Adjustments to reconcile net loss to net cash provided by operating activities:		
Depreciation and amortization	12,081	8,075
Stock-based compensation	73,368	73,540
Amortization of deferred commissions	29,307	24,785
Deferred income taxes	489	604
Other	1,850	(375)
Changes in operating assets and liabilities:		
Accounts receivable	57,429	12,031
Deferred commissions	(26,595)	(21,449)
Prepaid expenses and other assets	13,783	(7,824)
Accounts payable	(861)	(489)
Accrued expenses and other liabilities	(80,384)	(36,813)
Deferred revenue	43,075	89,674
Net cash provided by operating activities	81,689	39,655
Cash flows from investing activities:		
Purchases of property and equipment	(4,277)	(2,850)
Capitalized internal-use software	(3,799)	(3,465)
Purchases of investments	(291,957)	(120,162)
Maturities of investments	263,850	162,617
Payments for business combinations, net of cash acquired	—	(1,975)
Net cash (used in) provided by investing activities	(36,183)	34,165
Cash flows from financing activities:		
Proceeds from exercise of stock options	656	1,849
Proceeds from issuance of common stock under employee stock purchase plan	16,559	13,492
Net cash provided by financing activities	17,215	15,341
Effect of exchange rate on cash, cash equivalents, and restricted cash	(9,483)	8,751
Net increase in cash, cash equivalents, and restricted cash	53,238	97,912
Cash, cash equivalents, and restricted cash, beginning of period	392,740	193,594
Cash, cash equivalents, and restricted cash, end of period	\$ 445,978	\$ 291,506
Supplemental cash flow information:		
Cash paid for income taxes, net of refunds	\$ 9,922	\$ 1,531
Cash paid for interest	—	9,299
Non-cash investing and financing activities:		
Property and equipment received, included in payables and accrued but not paid	\$ 2,552	\$ 1,788
Stock-based compensation capitalized in internal-use software	\$ 2,439	\$ 1,567

The accompanying notes are an integral part of these unaudited condensed consolidated financial statements.

Rubrik, Inc.
NOTES TO CONDENSED CONSOLIDATED FINANCIAL STATEMENTS
(unaudited)

Note 1 – Description of Business

Rubrik, Inc. (“Rubrik” or the “Company”) is a security and artificial intelligence (“AI”) operations company, with a mission to secure and accelerate the world’s AI transformation. Rubrik built the Rubrik Security Cloud (“RSC”) suite with Zero Trust design principles to secure data across enterprise, cloud, SaaS, unstructured data, and identity providers. RSC delivers a cloud native SaaS platform that detects, analyzes, and remediates data security risks and unauthorized user activities. Rubrik launched Rubrik Agent Cloud in February 2026 to provide a comprehensive AI operations suite that can dynamically monitor, control, and remediate agentic actions. The Company was incorporated in December 2013 as ScaleData, Inc., a Delaware corporation, and changed its name to Rubrik, Inc. in October 2014. The Company is headquartered in Palo Alto, California.

Note 2 – Basis of Presentation and Summary of Significant Accounting Policies

Fiscal Year

The Company’s fiscal year ends on January 31. For example, references to fiscal 2027 and 2026 refer to the fiscal year ending January 31, 2027 and 2026, respectively.

Basis of Presentation and Principles of Consolidation

The accompanying unaudited condensed consolidated financial statements have been prepared in conformity with accounting principles generally accepted in the United States (“U.S. GAAP”) and applicable rules and regulations of the U.S. Securities and Exchange Commission (the “SEC”) regarding interim financial reporting. Accordingly, they do not include all disclosures normally required in annual consolidated financial statements prepared in accordance with U.S. GAAP. Therefore, these unaudited condensed consolidated financial statements should be read in conjunction with the audited consolidated financial statements and notes included in the Company’s Annual Report on Form 10-K for the fiscal year ended January 31, 2026, as filed with the SEC on March 19, 2026 (the “Annual Report”).

The unaudited condensed consolidated financial statements and notes include the Company and its wholly-owned subsidiaries and reflect all adjustments that, in the opinion of management, are necessary for a fair presentation of the periods presented. All intercompany accounts and transactions have been eliminated in consolidation.

Certain prior period amounts reported in the unaudited condensed consolidated financial statements and notes have been reclassified to conform to the current year presentation. For the three months ended April 30, 2026 and 2025, the Company combined maintenance revenue and other revenue into “Other” on the unaudited condensed consolidated statements of operations. The presentation of cost of revenue has been conformed to reflect the changes related to the presentation of revenues. Such reclassifications related to the presentation of revenue and cost of revenue did not impact total revenue, loss from operations or net loss.

Use of Estimates

The preparation of unaudited condensed consolidated financial statements in conformity with U.S. GAAP requires management to make estimates and assumptions that affect the amounts reported in the unaudited condensed consolidated financial statements and accompanying notes. Such management estimates include, but are not limited to, the estimation of standalone selling prices for performance obligations, the estimates for material rights, the application of a portfolio approach for capitalization of deferred commissions, the determination of the period of benefit for deferred commissions, the determination of fair value of the Company’s common stock prior to the completion of the IPO, the valuation of stock-based awards, the valuation and assessment of recoverability of intangible assets and their estimated useful lives, the assessment of goodwill impairment, the incremental borrowing rate used to value operating lease liabilities, the valuation of deferred income tax assets and uncertain tax positions, and contingencies. Management evaluates these estimates and assumptions on an ongoing basis using historical experience and other factors and makes adjustments when facts and circumstances dictate. Actual results could differ materially from these estimates.

Revenue Recognition

The Company generates revenue primarily from the sale of subscriptions and typically invoices customers at the inception of the contract. The Company’s contracts with customers have a typical stated duration ranging from one to five years, with the majority of contracts having a stated duration of three years. The Company’s contracts with customers are generally non-cancelable and non-refundable. The Company primarily sells products and services to end users through distributors and resellers (“Channel Partners”). Channel Partners are the Company’s customers. The Company offers rebates to its Channel Partners calculated as a fixed percentage

of the total selling price of a revenue contract. The Company accounts for rebates as consideration payable to a customer and records the amounts as a reduction to revenue.

The Company determines revenue recognition through the following steps:

- Identification of the contract, or contracts, with a customer;
- Identification of the performance obligations in the contract;
- Determination of the transaction price;
- Allocation of the transaction price to the performance obligations in the contract; and
- Recognition of revenue when, or as, the Company satisfies a performance obligation.

Payment terms of the Company's contracts range from 30 days to 60 days after fulfillment or service commencement date, except for certain contracts, which are billed in installments over the contract term.

The Company determines its transaction price based on the expected amount it is entitled to receive in exchange for transferring promised products and services to the customer.

The Company's contracts with customers can include multiple products and services. The Company determines performance obligations in a customer contract by assessing whether products and services are capable of being distinct and distinct in the context of the contract, including customer options that are determined to be material rights. The transaction price is allocated to the separate performance obligations based on the relative standalone selling price basis. The standalone selling price is determined based on the price at which the performance obligation either is sold separately or, if not observable through past transactions, is estimated taking into account available information such as market conditions and internally approved pricing guidelines related to the performance obligations. For performance obligations that are not sold separately, standalone selling price is determined based on observable inputs, overall pricing trends, market conditions and other factors, such as the price charged by the Company's competitors for similar products and services with any necessary or appropriate adjustments.

Subscription revenue

Subscription revenue consists of software-as-a-service ("SaaS") subscriptions and subscription term-based licenses with related support services.

SaaS subscriptions include standalone sales of SaaS subscription offerings as well as sales of RSC. RSC is a fully-hosted subscription in the case of protection of cloud, SaaS, and unstructured data applications. When RSC is securing enterprise applications, it is a hybrid cloud subscription which includes software hosted from the cloud (as a service) and on-premise software licenses. RSC is accounted for as a single performance obligation because the software hosted from the cloud (as a service) and the on-premise software licenses are not separately identifiable and serve together to fulfill the Company's promise to RSC customers, which is to provide a single, unified data security solution. The Company's subscription capabilities are primarily sold as editions which bundle multiple products and include the Foundation Edition, Business Edition, and Enterprise Edition. Subscription revenue related to SaaS is recognized ratably over the subscription period.

Subscription term-based licenses provide customers with a right to use the software for a fixed term commencing upon delivery of the license to the customers. Support services are bundled with each subscription term-based license for the term of the subscription. Subscription revenue related to subscription term-based licenses includes upfront revenue recognized at the later of the start date of the subscription term-based license and the date when the subscription term-based license is delivered. The remainder of the revenue is recognized ratably over the subscription period for support services, commencing on the date the service is made available to customers. The Company does not recognize software revenue related to the renewal of subscription term-based licenses earlier than the beginning of the related renewal period. The Company also sells Rubrik-branded commodity servers ("Rubrik-branded Appliances") support which is recognized ratably over the support period.

Other revenue

Other revenue includes fees earned from sales of professional services, software updates on a when-and-if-available basis, telephone and integrated web-based support, Rubrik-branded Appliance maintenance relating to our perpetual licenses, and Rubrik-branded Appliances. Revenue related to professional services is typically recognized as the services are performed. Revenue for Rubrik-branded Appliances is recognized when shipped to the customer, as the Company's shipping term is free on board shipping point, meaning control of the Rubrik-branded Appliance transfers to the customer upon shipment. When we sell our software license with our Rubrik-branded Appliances, revenue for both the Rubrik-branded Appliances and software licenses are recognized at the same time.

Amounts billed to customers for shipping and handling costs are classified as other revenue, and the Company's shipping and handling costs are classified as cost of revenue.

Judgments

The Company identifies performance obligations in a customer contract by assessing whether products and services are capable of being distinct and distinct in the context of the contract. The determination of the performance obligations for RSC when offered as a hybrid cloud subscription requires significant judgment due to the ongoing interaction between the software hosted from the cloud (as a service) and the on-premise software licenses. The Company has concluded that the software hosted from the cloud (as a service) and software licenses are not distinct from each other in the context of the contract such that revenue from the combined offering should be recognized ratably over the subscription period for which the software hosted from the cloud (as a service) is provided. In reaching this conclusion, the Company considered the nature of its promise to customers with a RSC hybrid cloud subscription, which is to provide a single, unified data security solution that operates seamlessly across multiple data sources and teams, and to give customers the ability to manage all their data sources consistently and/or in a manner they dictate. The Company only fulfills this multi-faceted promise by providing access to an integrated solution comprised of both cloud-based and on-premise software. The cloud-based software and on-premise software work together to provide features and functionalities necessary to fulfill that promise, which neither the software hosted from the cloud (as a service) nor the software licenses could provide on their own or together with third-party resources.

The Company had offered Subscription Credits for RSC to qualified customers in exchange for relinquishing their existing rights to next-generation Rubrik-branded Appliances at no cost ("Refresh Rights"). These are customer options that are accounted for as material rights.

The Company's contracts with customers may include customer options that are material rights. The determination of the likelihood of customers exercising their options requires significant judgment. Management estimates the likelihood of customers exercising their options by taking into account available information such as the number and timing of options exercised or forfeited, and considers other factors such as customer churn that may impact the options that have yet to be exercised or forfeited. Depending on the type of customer option exercised, the amount of consideration allocated to the material rights will be recognized into revenue at a point in time or over time beginning on the date the customer accepts the option. Deferred revenue associated with customer options that are subsequently forfeited will be released into revenue at the time the options are forfeited.

Timing of revenue recognition (in thousands):

	Three Months Ended April 30,	
	2026	2025
Subscription revenue		
Products and services transferred over time	\$ 355,639	\$ 243,991
Products and services transferred at a point in time	18,514	21,670
Other revenue		
Products and services transferred over time	11,160	11,074
Products and services transferred at a point in time	1,755	1,746
Total revenue	<u>\$ 387,068</u>	<u>\$ 278,481</u>

Contract assets

The Company invoices its customers in accordance with contractual billing terms established in each contract. As the Company performs under customer contracts, its right to consideration that is unconditional is classified as accounts receivable. If the Company's right to consideration for such performance is contingent upon a future event or satisfaction of additional performance obligations, the amount of revenue the Company has recognized in excess of the amount it has billed to the customer is classified as a contract asset. Contract assets are included in prepaid expenses and other current assets and other assets, noncurrent in the unaudited condensed consolidated balance sheets. There were \$14.0 million and \$12.6 million of contract assets as of April 30, 2026 and January 31, 2026, respectively. The current and noncurrent contract assets balances as of April 30, 2026 were \$4.6 million and \$9.4 million, respectively, and as of January 31, 2026 were \$3.8 million and \$8.8 million, respectively.

Deferred revenue

Deferred revenue, which are contract liabilities, are amounts received or due from customers in advance of the Company's performance. The current portion of deferred revenue represents the amount that is expected to be recognized as revenue within one year of the unaudited condensed consolidated balance sheet date. The Company invoices customers upfront for the majority of contracts, and the increase in the Company's deferred revenue corresponds to an increase in revenue contracts that include SaaS and support in which the Company satisfies its performance obligations typically over the contractual service period. During the three

months ended April 30, 2026 and 2025, the Company recognized revenue of approximately \$336.4 million and \$240.3 million, respectively, pertaining to amounts deferred at the beginning of each respective period.

Transaction price allocated to the remaining performance obligations

Transaction price allocated to the remaining performance obligations represents contracted revenue that has not yet been recognized, which includes deferred revenue for contracts that have been invoiced and will be recognized as revenue in future periods.

As of April 30, 2026, total remaining non-cancellable performance obligations under the Company's contracts with customers was approximately \$2.44 billion. The Company expects to recognize approximately 53% of this amount as revenue over the next 12 months, with the remaining balance to be recognized as revenue thereafter.

Concentration of Risk

Credit risk

The Company's financial instruments that are exposed to concentrations of credit risk consist primarily of cash and cash equivalents, restricted cash, short-term investments, and accounts receivable. Cash and cash equivalents and short-term investments are primarily held in three financial institutions and, at times, may exceed federally insured limits. The Company grants credit to customers in a wide variety of industries worldwide and generally does not require collateral. The Company has not experienced any material credit losses as of April 30, 2026.

Concentration of revenue and accounts receivable

The following customers individually accounted for 10% or more of total revenue or 10% or more of accounts receivable, net:

	Revenue		Accounts Receivable, Net	
	Three Months Ended April 30,		April 30,	January 31,
	2026	2025	2026	2026
Partner A	27%	29%	24%	32%
Partner B	29%	32%	26%	21%
Partner C	*	*	11%	*
Partner D	*	*	*	11%
Partner E	*	*	12%	*

* Less than 10%

Vendor risk

The Company uses third-party vendors for delivering its SaaS. While these services are highly available and designed to be resilient to failure of infrastructure, the Company's services could be significantly impacted if the third-party vendors' services experience certain types of interruptions.

Recent Accounting Pronouncements

Recently Adopted Accounting Pronouncements

In July 2025, the FASB issued ASU 2025-05, Financial Instruments — Credit Losses, which provides a practical expedient for estimating expected credit losses for current accounts receivable and current contract assets that arise from transactions accounted for under Topic 606, Revenue from Contracts with Customers. The Company adopted ASU 2025-05 effective February 1, 2026 on a prospective basis and elected the practical expedient. The adoption did not have a material impact on the Company's unaudited condensed consolidated financial statements and related disclosures.

Recently Announced Accounting Pronouncements Not Yet Adopted

In November 2024, the FASB issued ASU 2024-03, Income Statement - Reporting Comprehensive Income - Expense Disaggregation Disclosures, which requires entities to provide disclosures about specific types of expenses included in the expense captions presented on the face of the income statement as well as disclosures about selling expenses. ASU 2024-03 is effective for annual periods beginning after December 15, 2026, and interim periods beginning after December 15, 2027, on either a prospective or retrospective basis, with early adoption permitted. The Company is assessing the timing and impact of adopting this standard.

In September 2025, the FASB issued ASU 2025-06, Intangibles - Goodwill and Other - Internal-Use Software: Targeted Improvements to the Accounting for Internal-Use Software, which modernizes the accounting for internal-use software costs by increasing the operability of the recognition guidance considering different methods of software development. ASU 2025-06 is effective for annual

periods beginning after December 15, 2027 and interim periods within those annual reporting periods and can be applied prospectively, retrospectively, or with a modified transition approach, with early adoption permitted. The Company is assessing the impact of adopting this standard.

Note 3 – Revenue by Geography

The geographic regions are the Americas, EMEA (Europe, the Middle East, and Africa) and APAC (Asia Pacific). The following table sets forth revenue by geographic area based on ship to address (in thousands):

	Three Months Ended April 30,	
	2026	2025
Americas	\$ 278,913	\$ 202,765
EMEA	\$ 92,188	64,760
APAC	\$ 15,967	10,956
Total revenue	\$ 387,068	\$ 278,481

For the three months ended April 30, 2026 and 2025, United States accounted for \$268.2 million and \$195.3 million, respectively, or 69% and 70%, respectively, of consolidated total revenue.

Note 4 – Intangible Assets

Acquired intangible assets are as follows (in thousands):

	April 30, 2026		
	Gross	Accumulated Amortization	Net
Acquired technology	\$ 28,641	\$ (15,640)	\$ 13,001
Total	\$ 28,641	\$ (15,640)	\$ 13,001

	January 31, 2026		
	Gross	Accumulated Amortization	Net
Acquired technology	\$ 28,641	\$ (12,838)	\$ 15,803
Total	\$ 28,641	\$ (12,838)	\$ 15,803

The Company recognized \$2.8 million and \$1.0 million amortization expense in acquired intangible assets for the three months ended April 30, 2026 and 2025, respectively.

The following table summarizes the estimated future amortization expense of the acquired intangible assets as of April 30, 2026 (in thousands):

Fiscal year	Amount
Remainder of 2027	\$ 7,014
2028	4,513
2029	1,474
Total	\$ 13,001

Note 5 – Fair Value of Financial Instruments

The Company classifies its financial instruments within the fair value hierarchy based on the lowest level of input that is significant to the fair value measurement. Three levels of input may be used to measure fair value:

- Level 1 – Observable inputs are unadjusted quoted prices in active markets for identical assets or liabilities.
- Level 2 – Observable inputs are quoted for similar assets and liabilities in active markets or inputs other than quoted prices which are observable for the assets or liabilities, either directly or indirectly through market corroboration, for substantially the full term of the financial instruments.

[Table of Contents](#)

- Level 3 – Unobservable inputs that are supported by little or no market activity and are significant to the fair value of the assets or liabilities. These inputs will be based on the Company's own assumptions and will require significant management judgment or estimation.

The Company did not have any level 3 investments as of April 30, 2026 and January 31, 2026. The following table summarizes the Company's cash and available-for-sale marketable securities' amortized cost, gross unrealized gains, gross unrealized losses, and estimated fair value by significant investment category reported as cash and cash equivalents or short-term investments (in thousands):

April 30, 2026	Amortized Cost	Gross Unrealized Gains	Gross Unrealized Losses	Estimated Fair Value	Reported as	
					Cash and Cash Equivalents	Short-Term Investments
Cash:	\$ 67,343	\$ —	\$ —	\$ 67,343	\$ 67,343	\$ —
Level 1:						
Money market funds	359,989	—	—	359,989	359,989	—
U.S. Treasuries	549,393	139	(1,457)	548,075	2,065	546,010
Subtotal	909,382	139	(1,457)	908,064	362,054	546,010
Level 2:						
Certificate of deposit	8,216	5	(2)	8,219	—	8,219
Commercial paper	32,627	3	(15)	32,615	—	32,615
Corporate bonds	722,364	516	(613)	722,267	—	722,267
U.S. government agencies	10,597	9	—	10,606	—	10,606
Subtotal	773,804	533	(630)	773,707	—	773,707
Total	\$ 1,750,529	\$ 672	\$ (2,087)	\$ 1,749,114	\$ 429,397	\$ 1,319,717

January 31, 2026	Amortized Cost	Gross Unrealized Gains	Gross Unrealized Losses	Estimated Fair Value	Reported as	
					Cash and Cash Equivalents	Short-Term Investments
Cash:	\$ 66,674	\$ —	\$ —	\$ 66,674	\$ 66,674	\$ —
Level 1:						
Money market funds	294,365	—	—	294,365	294,365	—
U.S. Treasuries	539,437	627	(101)	539,963	6,054	533,909
Subtotal	833,802	627	(101)	834,328	300,419	533,909
Level 2:						
Certificate of Deposit	19,949	8	—	19,957	9,816	10,141
Commercial paper	39,994	16	—	40,010	3,287	36,723
Corporate bonds	702,250	1,958	(4)	704,204	—	704,204
U.S. government agencies	10,585	17	—	10,602	—	10,602
Subtotal	772,778	1,999	(4)	774,773	13,103	761,670
Total	\$ 1,673,254	\$ 2,626	\$ (105)	\$ 1,675,775	\$ 380,196	\$ 1,295,579

The following table summarizes the estimated fair value of the Company's investments by their remaining contractual maturity dates (in thousands):

	April 30, 2026
Due within one year	\$ 708,224
Due between one to two years	611,493
Total	\$ 1,319,717

For available-for-sale debt securities that have unrealized losses, the Company evaluates whether (i) the Company has the intention to sell any of these investments, (ii) it is not more likely than not that the Company will be required to sell any of these available-for-sale debt securities before recovery of the entire amortized cost basis, and (iii) the decline in the fair value of the investment is due to credit or non-credit related factors. Based on this evaluation, the Company determined that for its short-term investments there were no material credit or non-credit related impairments as of April 30, 2026 and January 31, 2026.

Convertible Notes

As of April 30, 2026, the total estimated fair value of the Convertible Notes (as defined below) was \$1.03 billion. The fair value was determined based on the quoted price of the Convertible Notes in an inactive market on the last trading day of the reporting period and is classified within Level 2 of the fair value hierarchy. See Note 7, Debt.

Note 6 – Balance Sheet Components

Prepaid Expenses and Other Current Assets

Prepaid expenses and other current assets consisted of the following (in thousands):

	April 30, 2026	January 31, 2026
Prepaid expenses	\$ 139,142	\$ 155,901
Inventory, net	7,043	5,676
Contract assets, current	4,645	3,845
Other current assets	14,538	14,943
Total prepaid expenses and other current assets	<u>\$ 165,368</u>	<u>\$ 180,365</u>

Property and Equipment, Net

Property and equipment, net consisted of the following (in thousands):

	April 30, 2026	January 31, 2026
Equipment	\$ 99,097	\$ 87,483
Capitalized internal-use software	59,503	53,265
Leasehold improvements	21,930	28,335
Furniture and fixtures	7,018	7,030
Total property and equipment, gross	187,548	176,113
Less: accumulated depreciation and amortization	(101,044)	(92,283)
Total property and equipment, net	<u>\$ 86,504</u>	<u>\$ 83,830</u>

Depreciation expense related to the Company's property and equipment, which did not include amortization expense related to capitalized internal-use software, was \$5.1 million and \$4.4 million for the three months ended April 30, 2026 and 2025, respectively.

Amortization expense relating to capitalized internal-use software was \$4.2 million and \$2.7 million for the three months ended April 30, 2026 and 2025, respectively.

Accrued Expenses and Other Current Liabilities

Accrued expenses and other current liabilities consisted of the following (in thousands):

	April 30, 2026	January 31, 2026
Accrued expenses	\$ 49,270	\$ 60,257
Accrued bonuses	17,957	56,630
Accrued sales commissions	16,153	36,958
Accrued payroll-related expenses, taxes, and benefits	40,816	58,170
Operating lease liabilities	14,612	12,709
Other	5,102	5,252
Total accrued expenses and other current liabilities	<u>\$ 143,910</u>	<u>\$ 229,976</u>

Note 7 – Debt

Convertible Notes

In June 2025, the Company issued \$1.15 billion aggregate principal amount of 0.00% convertible senior notes due 2030 (the "Convertible Notes" or "Notes"). Refer to Note 8, Debt of our Annual Report on Form 10-K for the fiscal year ended January 31, 2026, for additional information on the Convertible Notes.

As of April 30, 2026, the conditions allowing holders of the Convertible Notes to convert have not been met.

The net carrying amount of the Convertible Notes was as follows (in thousands):

		April 30, 2026
Principal	\$	1,150,000
Unamortized debt discount and issuance costs		(18,209)
Net carrying amount	\$	1,131,791

For the three months ended April 30, 2026, amortization of debt discount and issuance costs was \$1.1 million. The debt discount and issuance costs are being amortized into interest expense on the unaudited condensed consolidated statements of operations over the term of the Convertible Notes at an effective interest rate of 0.19%.

Capped Calls

In connection with the pricing of the Convertible Notes and the exercise in full by the initial purchasers of their option to purchase additional Convertible Notes, the Company entered into capped call transactions (the “Capped Calls”) with certain affiliates of certain initial purchasers of the Convertible Notes and other financial institutions. Refer to Note 8, Debt of our Annual Report on Form 10-K for the fiscal year ended January 31, 2026, for additional information on the Capped Calls.

Note 8 – Commitments and Contingencies

Purchase Commitments

As of April 30, 2026, there were no significant changes outside the ordinary course of business to the Company's commitments and purchase obligations since January 31, 2026.

Litigation

From time to time, the Company receives inquiries and/or claims or is involved in legal disputes and/or matters. In the opinion of management, any liabilities resulting from these claims will not have a material adverse effect on the Company's results of operations, financial position, and cash flows.

Warranties and Indemnifications

The Company provides to qualifying customers a services warranty program for recovery of certain expenses related to data recovery and restoration in the event that data backed up using the Company's solutions cannot be recovered following a ransomware attack. To date, costs relating to the warranty program have not been material.

The Company typically provides indemnification to customers for certain losses suffered or expenses incurred as a result of third-party claims arising from the Company's infringement of a third-party's intellectual property. Certain of these indemnification provisions survive termination or the expiration of the applicable agreement. The Company has not incurred a material liability relating to these indemnification provisions, and therefore, has not recorded a liability during any period for these indemnification provisions.

Note 9 – Stockholders’ Deficit

Equity Incentive Plan

The Company has reserved shares of its common stock for future issuance as follows (in thousands):

	April 30, 2026	January 31, 2026
2014 Stock Option and Grant Plan:		
Outstanding stock options	8,818	8,970
Outstanding restricted stock units	6,200	9,227
2024 Equity Incentive Plan:		
Outstanding restricted stock units	16,898	12,294
Shares available for future issuance under the 2024 Plan	64,061	58,406
2024 Employee Stock Purchase Plan	6,571	5,090
Total shares of common stock reserved	102,548	93,987

Stock Options

Options issued under the Company’s 2014 Plan and 2024 Plan generally are exercisable for periods not to exceed ten years and generally vest over four years with 25% vesting after one year and the remainder vesting monthly thereafter in equal installments.

A summary of the stock option activity and related information is as follows:

	Number of Options	Weighted- Average Exercise Price	Weighted- Average Remaining Contractual Term (years)	Aggregate Intrinsic Value (in thousands)
Outstanding as of January 31, 2026	8,970,353	\$ 29.20	7.6	\$ 239,954
Granted	—	—	—	—
Exercised	(152,660)	4.21	—	7,200
Cancelled	—	—	—	—
Outstanding as of April 30, 2026	8,817,693	\$ 29.63	7.4	\$ 207,630
Vested and exercisable as of April 30, 2026	3,649,981	\$ 26.28	6.7	\$ 98,168

There were no options granted during the three months ended April 30, 2026 and 2025.

The intrinsic value of the options exercised represents the difference between the estimated fair market value of the Company’s common stock on the date of exercise and the exercise price of each option.

As of April 30, 2026, there was approximately \$36.3 million of unrecognized stock-based compensation expense related to stock options, which is expected to be recognized over a weighted-average period of 1.7 years.

Restricted Stock Units

The Company grants service-based condition RSUs, service- and performance-based conditions RSUs, and service-, market-, and performance-based conditions RSUs. RSUs issued under the 2014 Plan and 2024 Plan typically have an expiry period of seven years from the grant date.

A summary of the RSU activity and related information is as follows:

	Number of RSUs	Weighted-Average Grant Date Fair Value
Unvested as of January 31, 2026	21,480,571	\$ 48.73
Granted	6,648,891	49.04
Vested	(2,840,496)	35.17
Forfeited	(2,191,311)	43.37
Outstanding as of April 30, 2026	23,097,655	\$ 51.00

For the three months ended April 30, 2026 and 2025, the total grant date fair value of vested RSUs was \$99.9 million and \$74.8 million, respectively.

As of April 30, 2026, there was approximately \$975.5 million of unrecognized stock-based compensation expense relating to RSUs, which is expected to be recognized over a weighted-average period of 1.6 years.

Restricted Stock

The Company issued 0.5 million shares of restricted stock in connection with the Predibase acquisition to certain Predibase employees with an aggregate fair value of \$40.4 million determined based on the closing price of \$88.11 per share of the Company's Class A common stock on July 18, 2025. These amounts are subject to vesting and continued employment, and will be recognized as stock-based compensation expense over the requisite service period of three years.

As of April 30, 2026, there was approximately \$29.6 million of unrecognized stock-based compensation expense relating to the restricted stock.

2024 Employee Stock Purchase Plan

The Company estimated the fair value of ESPP purchase rights using a Black-Scholes option-pricing model with the following assumptions:

	Three Months Ended April 30,	
	2026	2025
Expected term (in years)	0.5 - 2.0	0.5 - 2.0
Expected volatility	59.4% - 61.2%	59.0% - 64.7%
Risk-free interest rate	3.8% - 3.8%	3.9% - 4.3%
Dividend yield	—	—

As of April 30, 2026, there was approximately \$33.4 million of unrecognized stock-based compensation expense related to the ESPP, which is expected to be recognized over a weighted-average period of 1.3 years.

Stock-Based Compensation Expense

Total stock-based compensation expense included in the Company's unaudited condensed consolidated statements of operations was as follows (in thousands):

	Three Months Ended April 30,	
	2026	2025
Cost of revenue		
Subscription	\$ 4,631	\$ 3,968
Other	634	857
Research and development	33,026	19,812
Sales and marketing	16,331	24,144
General and administrative	18,746	24,759
Total stock-based compensation expense	<u>\$ 73,368</u>	<u>\$ 73,540</u>

Note 10 – Net Loss Per Share

For periods in which there were Class A and Class B shares outstanding, the rights, including the liquidation and dividend rights, of the holders of Class A and Class B common stock are identical, except with respect to voting, conversion, and transfer rights. As the liquidation and dividend rights are identical, the undistributed earnings are allocated on a proportionate basis to each class of common stock and the resulting basic and diluted net loss per share attributable to common stockholders are, therefore, the same for both Class A and Class B common stock on both individual and combined basis.

The following table presents the calculation of basic and diluted net loss per share (in thousands, except per share amounts):

	Three Months Ended April 30,			
	2026		2025	
	Class A	Class B	Class A	Class B
Numerator:				
Net loss	\$ (32,603)	\$ (9,250)	\$ (59,676)	\$ (42,428)
Denominator:				
Weighted-average common stock shares used in computing net loss per share, basic and diluted	158,655	45,013	111,998	79,627
Net loss per common stock share, basic and diluted	\$ (0.21)	\$ (0.21)	\$ (0.53)	\$ (0.53)

The following outstanding potentially dilutive securities were excluded from the computation of diluted net loss per share for the periods presented because the impact of including them would have been antidilutive (in thousands):

	Three Months Ended April 30,	
	2026	2025
Issued and outstanding stock options	8,818	9,373
Unvested RSUs issued and outstanding	23,098	24,105
Convertible notes	9,218	—
Restricted stock issued for business combination	396	—
Total	41,530	33,478

The Company entered into the Capped Calls in connection with the issuance of the Convertible Notes. The effect of the Capped Calls was excluded from the calculation of diluted net loss per share attributable to the Company's Class A common stockholders as the effect of the Capped Calls would have been antidilutive. The Capped Calls are generally expected to reduce the potential dilution to the Company's Class A common stock upon any conversion of the relevant series of the Convertible Notes. See Note 7, Debt.

Note 11 – Income Taxes

The Company recorded an income tax expense of \$4.6 million and \$1.3 million for the three months ended April 30, 2026 and 2025, respectively.

For the three months ended April 30, 2026 and 2025, the income tax provision consisted of taxes on the income of the Company's foreign subsidiaries, foreign withholding taxes, and U.S. state taxes, partially offset by excess benefits from stock-based compensation deductions in the UK.

As of April 30, 2026, the Company maintained a full valuation allowance on its U.S. federal and state net deferred tax assets as it was more likely than not that those deferred tax assets will not be realized.

Note 12 – Segment Reporting

The Company has one reportable segment which is software and services. The software and services segment provides unified data security solutions to customers primarily under SaaS arrangements. The Company manages the business activities on a consolidated basis. The technology used in the customer arrangements is primarily based on a single software platform that is deployed to and implemented by customers in a similar manner. The types of software and services from which the Company generates revenue are described under the "Revenue Recognition" policy within the "Note 2, Basis of Presentation and Summary of Significant Accounting Policies."

The Company's chief operating decision maker is its chief executive officer. The chief operating decision maker assesses performance for the software and services segment and decides how to allocate resources based on net loss that is also reported on the consolidated statements of operations as consolidated net loss. The chief operating decision maker does not use any segment assets measure to assess performance and decide how to allocate resources.

The chief operating decision maker uses net loss and the functional areas as a percentage of revenue to evaluate and decide where to invest within the software and services segment. Net loss is used to monitor budget versus actual results. The chief operating decision maker also uses net loss in competitive analysis by benchmarking to the Company's competitors. The competitive analysis along with the monitoring of budgeted versus actual results are used in assessing the performance of the segment.

[Table of Contents](#)

The Company does not have intra-entity sales or transfers.

The following table presents the segment information (in thousands):

	Three Months Ended April 30,	
	2026	2025
Total revenue	\$ 387,068	\$ 278,481
Less:		
Adjusted subscription cost of revenue ⁽¹⁾	58,194	46,635
Remaining cost of revenue	4,440	5,124
Remaining research and development expenses	78,875	59,883
Remaining sales and marketing expenses	175,278	144,404
Remaining general and administrative expenses	36,734	33,208
Stock-based compensation expense ⁽²⁾	73,368	73,540
Depreciation and amortization	10,011	7,818
Amortization of acquired intangibles	2,802	960
Interest expense	1,070	9,813
Income tax expense	4,637	1,274
Other items ⁽³⁾	(590)	5,622
Plus:		
Interest income	15,898	7,696
Segment net loss	(41,853)	(102,104)
Consolidated net loss	<u>\$ (41,853)</u>	<u>\$ (102,104)</u>

(1) Adjusted subscription cost of revenue is subscription cost of revenue adjusted for stock-based compensation expense, amortization of acquired intangibles, and stock-based compensation from amortization of capitalized internal-use software as follows (in thousands):

	Three Months Ended April 30,	
	2026	2025
Subscription cost of revenue	\$ 66,723	\$ 51,912
Less:		
Stock-based compensation expense	4,631	3,968
Amortization of acquired intangibles	2,802	960
Stock-based compensation from amortization of capitalized internal-use software	1,096	349
Adjusted subscription cost of revenue	<u>\$ 58,194</u>	<u>\$ 46,635</u>

(2) See Note 9 for stock-based compensation expense by captions.

(3) Other items include foreign currency exchange gains (losses).

Item 2. Management's Discussion and Analysis of Financial Condition and Results of Operations

The following discussion and analysis of our financial condition and results of operations should be read in conjunction with our unaudited condensed consolidated financial statements and related notes appearing elsewhere in this Quarterly Report on Form 10-Q and our audited consolidated financial statements and the related notes and the discussion under the heading "Management's Discussion and Analysis of Financial Condition and Results of Operations" included in the Company's Annual Report on Form 10-K for the fiscal year ended January 31, 2026, as filed with the SEC on March 19, 2026 (the "Annual Report"). Some of the information contained in this discussion and analysis includes forward-looking statements that involve risks and uncertainties as described under the heading "Special Note About Forward-Looking Statements" in this Quarterly Report on Form 10-Q. You should review the disclosure under the heading "Risk Factors" in this Quarterly Report on Form 10-Q for a discussion of important factors that could cause our actual results to differ materially from those anticipated in these forward-looking statements.

Unless the context otherwise requires, all references in this Quarterly Report on Form 10-Q to "we," "us," "our," "our company," and "Rubrik" refer to Rubrik, Inc. and its consolidated subsidiaries. Unless otherwise indicated, references to our "common stock" include our Class A common stock and Class B common stock.

Overview

We are on a mission to secure and accelerate the world's AI transformation.

Cyberattacks are inevitable. Prevention and detection are not enough. Realizing that cyberattacks ultimately target data, we created Zero Trust Data Security to deliver cyber resilience so that organizations can secure their data across the cloud and recover from cyberattacks. As enterprises embrace the forthcoming AI transformation, they are grappling with a threat landscape that is now amplified at an AI-scale. We believe that cyber resilience will result in AI resilience and that the future of cybersecurity is data security—if your data is secure, your business is resilient.

We built the Rubrik Security Cloud ("RSC") suite with Zero Trust design principles to secure data across enterprise, cloud, SaaS, unstructured data, and identity providers. RSC delivers a cloud native SaaS platform that detects, analyzes, and remediates data security risks and unauthorized user activities. Our platform is architected to help organizations achieve cyber resilience, which encompasses cyber posture and cyber recovery. We enable organizations to confidently accelerate digital transformation and leverage the cloud to realize business agility.

We launched our first enterprise software product, Converged Data Management, in fiscal 2016, which combined data and metadata together into a single layer of software to offer Zero Trust data protection, and sold it as a perpetual license along with associated maintenance contracts. In fiscal 2019, we extended data protection to cloud native applications and rebranded Converged Data Management to Cloud Data Management ("CDM"). Data protection for cloud native applications are sold as a SaaS subscription offering. In addition, we began launching new SaaS subscription offerings, Anomaly Detection and Sensitive Data Monitoring. In fiscal 2020, we continued our business evolution to a subscription pricing model by offering CDM as a subscription term-based license with associated support. Included in this subscription term-based license was the right to next generation Rubrik-branded commodity servers ("Rubrik-branded Appliances") at no cost for qualified customers ("Refresh Rights"). As of February 1, 2022, we stopped offering CDM as a perpetual license.

In fiscal 2023, to meet customer demands for data security and a single, unified cloud-based control plane, we launched RSC, a suite built on top of our comprehensive Zero Trust Data Security platform. RSC culminates our early vision of providing one point of control to secure data across enterprise, cloud, SaaS, unstructured data, and identity providers. RSC is primarily adopted by our customers as a cloud-native, fully managed SaaS solution. It is also available as an enterprise-ready, self-managed version ("RSC-Private"), for a few select customers that are subject to stringent data control policies. For U.S. public sector organizations, we also offer a specialized cloud-native fully managed SaaS solution called RSC-Government.

We began transitioning customers from our legacy CDM capabilities to RSC, which is offered on a subscription basis, in fiscal 2023. As part of this business transition, we began transitioning the sale of Rubrik-branded Appliances from us to our contract manufacturers and stopped offering the Refresh Rights as part of our subscription offerings. In lieu of offering Refresh Rights, we offered Subscription Credits to qualifying customers (which are customer options that are accounted for as material rights). We recognize ratable revenue upon utilization or upfront revenue upon expiration of Subscription Credits, and utilization of Subscription Credits also offsets Subscription ARR for the applicable period. Since the end of fiscal 2024, RSC has represented a majority of our total revenue.

We recognize revenue from the sales of our RSC suite (excluding RSC-Private) ratably over the term of the subscription. We recognize a portion of revenue from sales of RSC-Private upon delivery and the remainder ratably over the term of the subscription. The majority of sales of our subscriptions are for three-year terms with upfront payment, and renewals are typically for one-year terms.

New and existing customers have largely adopted RSC. We have largely migrated our existing customers from our legacy CDM capabilities to RSC. During this migration, certain existing customers consumed our platform and products through a mix of RSC and a transitional CDM license ("RCDM-T"), during which time we recognized a portion of the associated revenue from these customers upfront at the time we transferred control of the license to the customer, and we have largely completed this transition in fiscal 2026. In addition, we expect our subscription revenue to continue to benefit from customers exercising or forfeiting their Subscription Credits through fiscal 2027, although we expect the benefits to significantly decline sequentially.

In fiscal 2026, we launched RAC, our AI agent operations suite, to accelerate enterprise AI transformation without introducing added risk. RAC is designed to monitor and audit agentic actions, enforce real-time guardrails for agentic changes, fine-tune agents for accuracy and, finally, undo agent mistakes. Built on our unique architecture that understands data, identity and application contexts, RAC is designed to give customers security, accuracy, and efficiency as they transform their organizations into AI enterprises. As RAC only became commercially available in February of 2026, we expect the RSC suite to continue to be the majority of our revenue in fiscal 2027 and the main driver for ARR growth.

In the first quarter of fiscal 2027, we started offering the Resilience Guardian as a term-based subscription license program, which provides customers with dedicated resilience managers to design and implement a cyber resilience strategy that maps to business outcomes. This includes proactive security and health checks, detection and resolution of emerging issues, upgrade planning and assistance, and adoption excellence and value realization.

Factors Affecting Our Performance

Evolution of the Market and Adoption of Our Solutions

Our future success depends in part on the market adoption of our approach to Zero Trust Data Security. Many organizations have focused on preventing cyberattacks instead of protecting their data and having a plan to recover it in case of a cyberattack. We believe that the existing security ecosystem lacks a data security platform that will secure a customer's data, wherever it lives, across enterprise, cloud, SaaS, unstructured data, and identity providers. RSC is our Zero Trust Data Security platform that addresses the growing demand from organizations of virtually any size, across a wide range of industries, to address data security and cyberattack risks. As the data security market continues to evolve, we expect to continuously innovate our platform and product functionality to keep us in a strong position to capture the large opportunity ahead.

New Customer Acquisition

Our business model relies on rapidly and efficiently engaging with new customers. Our ability to attract new customers will depend on a number of factors, including our ability to innovate upon our product breadth and capabilities, our success in recruiting and scaling our sales and marketing organization, our ability to accelerate ramp time of our sales force, our ability to develop and maintain strong partnerships, the impact of marketing efforts to enhance our brand, and competitive dynamics in our target markets.

Retaining and Expanding Within Our Existing Customer Base

Our ability to retain customers and expand within existing customers is integral to our growth and future success. Our growing base of customers represents a significant opportunity for further expansion across our platform. Our customers typically start with securing data in one or more applications on our platform, and then expand by securing additional applications and increasing the amount of data secured. They further extend their use of our platform through adoption of additional security products. Several of our largest customers have deployed our platform to secure large amounts of their data across enterprise, cloud, SaaS, unstructured data, and identity providers. Our ability to expand and extend within our customer base depends on, and has been impacted by, a number of factors, including platform performance, our customers' satisfaction with our platform, competitive offerings, pricing, overall changes in our customers' spending levels, and the effectiveness of our efforts to help our customers realize the benefits of our platform.

Macroeconomic and Supply Chain Conditions

Our overall performance depends in part on worldwide economic and geopolitical conditions and their impact on customer behavior. Macroeconomic conditions, including inflation, fluctuations in interest rates, foreign currency fluctuations, tariffs or other trade restrictions, geopolitical issues, changes in government policy or spending, and other changes in economic conditions, may adversely affect the buying patterns of our customers and prospective customers. For example, in light of current macroeconomic conditions, such as higher cost-consciousness around information technology budgets, as well as constraints affecting the availability or pricing of compatible commodity servers needed to deploy our solutions, we have observed a lengthening of our sales cycles. Additionally, key components of the commodity servers that are compatible with our solutions have been, and continue to be, affected by global chip shortages and allocation constraints, in part due to elevated industry demand, which in certain cases have resulted in extended lead times and increased server prices. Such delays, constraints and increased costs may affect our customers' purchasing decisions and

deployment timelines, in some cases delaying customer purchases and in other cases resulting in customers pulling software purchases forward to lock in hardware prices. In response, we may in the future provide certain commercial accommodations, which could reduce our margins or adversely affect our revenue and operating results if such practices become widespread or prolonged. Due to our subscription-focused business model, any impact of the current macroeconomic environment and supply chain constraints on our business may not be fully reflected in our results of operations until future periods. As we continue to monitor the direct and indirect impacts of the current environment, the broader implications of macroeconomic conditions and supply chain constraints on our business, results of operations and financial condition, particularly in the long term, remain uncertain.

Key Business Metrics

We monitor the following key business metrics to help us evaluate our business.

Subscription ARR

Subscription ARR is calculated as the annualized value of our active subscriptions as of the measurement date, based on our customers' total contract value, and assuming any contract that expires during the next 12 months is renewed on existing terms. Subscriptions include offerings for our RSC suite and related data security SaaS solutions, term-based licenses for our RSC-Private suite and related products, prior sales of CDM sold as a subscription term-based license with associated support and related SaaS products, and standalone sales of our SaaS subscription offerings like Anomaly Detection, Sensitive Data Monitoring and Resilience Guardian. We believe Subscription ARR illustrates our success in acquiring new subscription customers and maintaining and expanding our relationships with existing subscription customers.

The following table sets forth our Subscription ARR as of the dates presented:

	April 30,	
	2026	2025
	(in thousands, except percentages)	
Subscription ARR	\$ 1,565,141	\$ 1,181,269
% growth	32 %	38 %

Subscription ARR does not include any maintenance revenue associated with perpetual licenses, which we generally no longer offer. Of the 32% and 38% growth, approximately 0.4 percentage points and 2 percentage points of growth for the three months ended April 30, 2026 and 2025, respectively, were a result of transitioning our existing maintenance customers to our subscription editions. Contributions to growth from these transitions were largely completed in fiscal 2026.

Cloud Annual Recurring Revenue, or Cloud ARR

Cloud ARR is calculated as the annualized value of our active cloud-based subscriptions as of the measurement date, based on our customers' total contract value, and assuming any contract that expires during the next 12 months is renewed on existing terms. Our cloud-based subscriptions include RSC and RSC-Government (excluding RSC-Private). Cloud ARR also includes SaaS subscription offerings like Anomaly Detection and Sensitive Data Monitoring, which are sold standalone or with prior sales of term-based license offerings of CDM. We believe that Cloud ARR provides important information on new and existing customers purchasing new RSC subscription offerings and existing subscription term-based license customers renewing with RSC subscription offerings.

The following table sets forth our Cloud ARR as of the dates presented:

	April 30,	
	2026	2025
	(in thousands, except percentages)	
Cloud ARR	\$ 1,393,920	\$ 971,546
% growth	43 %	60 %

Average Subscription Dollar-Based Net Retention Rate

Our average subscription dollar-based net retention rate compares our Subscription ARR from the same set of subscription customers across comparable periods. We calculate our average subscription dollar-based net retention rate by first identifying subscription customers (the "Prior Period Subscription Customers") that were subscription customers at the end of a particular quarter (the "Prior Period") and calculate the Subscription ARR from the Prior Period Subscription Customers. We then calculate the Subscription ARR from these Prior Period Subscription Customers at the end of the same quarter of the subsequent year (the "Current Period"). This

calculation captures upsells, contraction, and attrition since the Prior Period. We then divide total Current Period Subscription ARR by the total Prior Period Subscription ARR for Prior Period Subscription Customers. Our average subscription dollar-based net retention rate in a particular quarter is obtained by averaging the result from that particular quarter with the corresponding results from each of the prior three quarters. We believe that our average subscription dollar-based net retention rate provides useful information about the evolution of our existing customers as they expand through the increase of data from applications we already secure, new applications for us to secure, additional data security products, and conversion of our recurring revenue related to maintenance contracts into subscription revenue.

Our historical average subscription dollar-based net retention rate does not include any maintenance revenue associated with perpetual licenses, which we no longer offer. Like Subscription ARR, our historical average subscription dollar-based net retention rate benefits from the transition of our existing maintenance customers to our subscription editions.

The following table sets forth our average subscription dollar-based net retention rate as of the dates presented:

	April 30,	
	2026	2025
Average subscription dollar-based net retention rate	approximately 120%	over 120%

Customers with \$100,000 or More in Subscription ARR

We believe that customers with \$100,000 or more in Subscription ARR is a helpful metric in measuring our ability to scale with our customers and the success of our ability to acquire large customers. Additionally, we believe that our ability to increase the number of customers with \$100,000 or more in Subscription ARR is a useful indicator of our market penetration and demand for our platform.

The following table sets forth the number of customers with \$100,000 or more in Subscription ARR as of the dates presented:

	April 30,	
	2026	2025
Customers with \$100,000 or more in Subscription ARR	2,946	2,381
% growth	24 %	28 %

Non-GAAP Financial Measures

We believe that non-GAAP financial measures, when taken collectively, may be helpful to investors because they provide consistency and comparability with past financial performance. However, non-GAAP financial measures are presented for supplemental informational purposes only, have limitations as an analytical tool, and should not be considered in isolation or as a substitute for financial information presented in accordance with GAAP. Other companies, including companies in our industry, may calculate similarly titled non-GAAP financial measures differently or may use other measures to evaluate their performance, all of which could reduce the usefulness of our non-GAAP financial measures as tools for comparison. A reconciliation is provided below for each non-GAAP financial measure to the most directly comparable financial measure stated in accordance with GAAP. Investors are encouraged to review the related GAAP financial measures and the reconciliation of these non-GAAP financial measures to their most directly comparable GAAP financial measures, and not to rely on any single financial measure to evaluate our business.

Free Cash Flow

Free cash flow is a non-GAAP financial measure that we calculate as net cash provided by (used in) operating activities less cash used for purchases of property and equipment and capitalized internal-use software. We believe that free cash flow is a helpful indicator of liquidity that provides information to management and investors about the amount of cash generated or used by our operations that, after the investments in property and equipment and capitalized internal-use software, can be used for strategic initiatives, including investing in our business and strengthening our financial position. The limitation of free cash flow is that it does not reflect our future contractual commitments and may fluctuate due to the timing of cash payments received from our customers and payments relative to expenses, prepayments of other spend, including hosting prepayments, and charitable donations. Additionally, free cash flow is not a substitute for cash provided by (used in) operating activities, and the utility of free cash flow as a measure of our liquidity is further limited as it does not represent the total increase or decrease in our cash balance for a given period.

Free cash flow was \$73.6 million and \$33.3 million for the three months ended April 30, 2026 and 2025, respectively. The improvement in free cash flow was primarily due to higher sales, including timing of renewals, improved operating leverage and optimizing our capital structure. This trend when combined with changes in new business growth, may result in free cash flow volatility across periods.

In the longer term, we view continued Subscription ARR growth, operating leverage, and the mix of annual versus upfront payment terms on our multi-year contracts as primary drivers of free cash flow. See the risk factor titled “We expect fluctuations in our financial results, making it difficult to project future results, and if we fail to meet the expectations of securities analysts or investors with respect to our results of operations, our stock price and the value of your investment could decline” in the section titled “Risk Factors.”

The following table presents a reconciliation of free cash flow to net cash provided by operating activities for the periods presented:

	Three Months Ended April 30,	
	2026	2025
	(in thousands)	
Net cash provided by operating activities	\$ 81,689	\$ 39,655
Less: Purchases of property and equipment	(4,277)	(2,850)
Less: Capitalized internal-use software	(3,799)	(3,465)
Free cash flow	\$ 73,613	\$ 33,340
Net cash (used in) provided by investing activities	\$ (36,183)	\$ 34,165
Net cash provided by financing activities	\$ 17,215	\$ 15,341

Subscription ARR Contribution Margin

We define Subscription ARR Contribution Margin as the Subscription ARR Contribution (as defined below) divided by Subscription ARR at the end of the period. We define Subscription ARR Contribution as Subscription ARR at the end of the period less: (i) our non-GAAP subscription cost of revenue and (ii) our non-GAAP operating expenses for the prior 12-month period ending on that date. In fiscal 2023, we began transitioning customers from our legacy CDM capabilities to our subscription-based RSC offerings. As a result of differing revenue recognition treatment between CDM and RSC, including the RCDM-T licenses offered to existing customers, and as qualified customers choose to exercise or forfeit their Subscription Credits, these business transitions cause fluctuations to our total revenue growth and limit the comparability of our revenue with past performance. As a result, we measure the performance of our business on the basis of Subscription ARR. We believe that Subscription ARR Contribution Margin is a helpful indicator of operating leverage during this business transition. One limitation of Subscription ARR Contribution Margin is that the factors that impact Subscription ARR will vary from those that impact subscription revenue and, as such, may not provide an accurate indication of our actual or future GAAP results. Additionally, the historical expenses in this calculation may not accurately reflect the costs associated with future commitments.

Subscription ARR Contribution Margin was 13% and 8% for the 12 months ended April 30, 2026 and 2025, respectively. The increase in Subscription ARR Contribution Margin was primarily driven by the strong year-over-year Subscription ARR growth outpacing the year-over-year growth in non-GAAP subscription costs of sales and non-GAAP operating expenses. We believe that this increase in Subscription ARR Contribution Margin reflects increased operating leverage in our business.

[Table of Contents](#)

The following table presents the calculation of Subscription ARR Contribution Margin for the periods presented as well as a reconciliation of (i) non-GAAP subscription cost of revenue to subscription cost of revenue and (ii) non-GAAP operating expenses to operating expenses:

	Twelve Months Ended April 30,	
	2026	2025
	(in thousands, except percentages)	
Subscription cost of revenue	\$ 244,552	\$ 193,223
Stock-based compensation expense	(17,037)	(18,289)
Stock-based compensation included in amortization of capitalized internal-use software	(2,903)	(607)
Amortization of acquired intangibles	(9,330)	(3,730)
Non-GAAP subscription cost of revenue	\$ 215,282	\$ 170,597
Operating expenses	\$ 1,453,058	\$ 1,249,744
Stock-based compensation expense	(309,832)	(334,156)
Non-GAAP operating expenses	\$ 1,143,226	\$ 915,588
Subscription ARR	\$ 1,565,141	\$ 1,181,269
Non-GAAP subscription cost of revenue	(215,282)	(170,597)
Non-GAAP operating expenses	(1,143,226)	(915,588)
Subscription ARR Contribution	\$ 206,633	\$ 95,084
Subscription ARR Contribution Margin	13.2 %	8.0 %

Components of Results of Operations

Revenue

We generate revenue primarily from sales of subscriptions and typically invoice our customers at the inception of the contract.

While we have largely completed both the sales of Rubrik-branded Appliances transitioning from us to our contract manufacturers in fiscal 2025 and the transition for new and existing customers to sales of RSC in fiscal 2026, we expect our subscription revenue to continue to benefit from customers exercising or forfeiting their Subscription Credits (which are customer options that are accounted for as material rights) through fiscal 2027, although we expect the benefits to significantly decline sequentially. These business transitions cause fluctuations to our total revenue growth and limit the comparability of our revenue with past performance. We primarily measure our business on the basis of Subscription ARR, as we believe it best reflects our actual growth and our growth prospects.

Certain prior period amounts reported in the unaudited condensed consolidated financial statements and notes have been reclassified to conform to the current year presentation. For the three months ended April 30, 2026 and 2025, the Company combined maintenance revenue and other revenue into "Other" on the unaudited condensed consolidated statements of operations. The presentation of cost of revenue has been conformed to reflect the changes related to the presentation of revenues. Such reclassifications related to the presentation of revenue and cost of revenue did not impact total revenue, loss from operations or net loss.

Subscription Revenue

Our subscription revenue consists of SaaS subscriptions and subscription term-based licenses with related support services.

SaaS includes SaaS subscription offerings like Anomaly Detection and Sensitive Data Monitoring sold standalone or with prior sales of term-based license offerings of CDM prior to the launch of the RSC suite as well as sales of RSC. RSC is offered as a fully-hosted subscription or a hybrid cloud subscription. RSC is a fully-hosted subscription in the case of protection of cloud, SaaS, unstructured data, and identity providers. When RSC is securing enterprise applications, it is a hybrid cloud subscription which includes software hosted from the cloud (as a service) and an on-premise license for securing enterprise applications. The hybrid cloud subscription is accounted for as a single performance obligation because the software hosted from the cloud (as a service) and the on-premise software licenses are not separately identifiable and serve together to fulfill our promise to the customer, which is to provide a single, unified data security solution. Our RSC subscription capabilities are primarily sold as editions which bundle multiple products and include the Foundation Edition, Business Edition, and Enterprise Edition. Subscription revenue related to SaaS is recognized ratably over the subscription period.

Subscription term-based licenses provide our customer with a right to use the software for a fixed term commencing upon delivery of the license to our customer. Support services are bundled with each subscription term-based license for the term of the subscription.

Subscription revenue related to subscription term-based licenses includes upfront revenue recognized at the later of the start date of the subscription term-based license and the date when the subscription term-based license is delivered. The remainder of the revenue is recognized ratably over the subscription period for support services, commencing with the date the service is made available to customers.

Our subscription revenue will fluctuate when qualified customers choose to exercise or forfeit their customer options that are accounted for as material rights. We have experienced revenue growth benefits from the non-recurring revenue associated with material rights; however, we expect these benefits to decline over the course of fiscal 2027. The combination of both of these factors may continue to limit and cause fluctuations in our subscription revenue growth during fiscal 2027, depending in part on the timing of our existing customers' transition to RSC and exercises or forfeitures of Subscription Credits (which are customer options that are accounted for as material rights).

Other Revenue

Other revenue includes fees earned from sales of professional services, software updates on a when-and-if-available basis, telephone and integrated web-based support, Rubrik-branded Appliance maintenance relating to our perpetual licenses, and Rubrik-branded Appliances. Revenue for Rubrik-branded Appliances is recognized when shipped to the customer. When we sell our software license with our Rubrik-branded Appliances, revenue for both the Rubrik-branded Appliances and software licenses are recognized at the same time. Revenue related to professional services is typically recognized as the services are performed. We expect other revenue to be largely driven by sales of professional services in the future and as a percentage of total revenue to decrease over time.

Cost of Revenue

Cost of revenue primarily includes employee compensation and related expenses associated with customer support, certain hosting costs, amortization of capitalized internal-use software, amortization of finite-lived intangible assets and cost of Rubrik-branded Appliances.

Cost of Subscription Revenue

Cost of subscription revenue primarily includes employee compensation and related expenses associated with customer support for our subscription offerings, certain hosting costs, amortization of capitalized internal-use software, and amortization of finite-lived intangible assets. We expect our cost of subscription revenue to increase as our subscription revenue increases.

Cost of Other Revenue

Cost of other revenue includes the cost of professional services, employee compensation and related expenses associated with customer support from our perpetual licenses, and the cost of Rubrik-branded Appliances. We expect cost of other revenue as a percentage of total cost of revenue to decrease as the transition of sales of Rubrik-branded Appliances from us to our contract manufacturers was largely completed in fiscal 2025. Over the long-term, we expect the cost of other revenue to be largely driven by sales of professional services.

Gross Profit and Margin

Gross profit is revenue less cost of revenue.

Gross margin is gross profit expressed as a percentage of revenue. Our gross margin has been, and will continue to be, affected by a number of factors, including the mix of subscription term-based licenses, SaaS subscriptions, and other products, when qualified customers choose to exercise or forfeit their customer options that are accounted for as material rights, the timing and extent of our investments in our global customer support organization, certain hosting costs, the amortization of capitalized internal-use software, and stock-based compensation expense. Over time, we expect our gross margin to fluctuate due to the factors described above.

Subscription Gross Margin

We expect our subscription gross margin to fluctuate through fiscal 2027. This is due to the revenue being recognized ratably over the subscription term rather than a portion being recognized upfront from subscription term-based licenses and associated increases in hosting costs for our SaaS solutions. We expect our subscription gross margin to fluctuate as customers adopt data security SaaS solutions on the RSC suite.

Other Gross Margin

We expect other gross margin to decrease as a percentage of total revenue, which we expect will result in a decrease in cost of other revenue. We expect sales of Rubrik-branded Appliances to decrease as the transition of sales of Rubrik-branded Appliances from us to

our contract manufacturers was largely completed in fiscal 2025. Over the long-term, we expect other gross margin to be largely driven by sales of professional services.

Operating Expenses

Our operating expenses consist of research and development, sales and marketing, and general and administrative expenses. Personnel costs are the most significant component of operating expenses. We also incur other non-personnel costs such as colocation and certain hosting costs, office space costs, fees for third-party professional services, and costs associated with software and subscription services. We expect our operating expenses will continue to increase as our business grows. We also expect our operating expenses, exclusive of stock-based compensation, as a percentage of revenue to generally decrease over the long term.

Research and Development

Research and development expenses consist primarily of employee compensation and related expenses, net of capitalized amounts, and colocation and certain hosting costs. To capture share in the ever-growing data security market, we expect to continuously innovate our platform and product functionality and will continue to invest in research and development. We expect our research and development expenses will continue to increase as our business grows. We also expect our research and development expenses, exclusive of stock-based compensation, as a percentage of revenue to generally decrease over the long term.

Sales and Marketing

Sales and marketing expenses consist primarily of employee compensation and related expenses including sales commissions, marketing programs, and travel-related costs. To capture share in the ever-growing data security market, we expect to continuously expand our sales force, increase our marketing efforts, and expand into new markets. We expect our sales and marketing expenses will continue to increase as our business grows. We also expect our sales and marketing expenses, exclusive of stock-based compensation, as a percentage of revenue to generally decrease over the long term.

General and Administrative

General and administrative expenses consist primarily of employee compensation and related expenses for administrative functions, including finance, legal, human resources, information technology, and fees for third-party professional services. We expect our general and administrative expenses will continue to increase as our business grows. We also expect our general and administrative expenses, exclusive of stock-based compensation, as a percentage of revenue to generally decrease over the long term.

Other Non-Operating Income (Expense)

Other non-operating income (expense) consists primarily of interest income, interest expense, loss on debt extinguishment, and foreign exchange gains and losses.

Income Tax Expense

Income tax expense consists primarily of income taxes in certain foreign jurisdictions in which we conduct business, as well as state income taxes in the United States. We have recorded U.S. federal and state net deferred tax assets for which we provide a full valuation allowance, which includes net operating loss carryforwards and tax credits. We expect to maintain this full valuation allowance for the foreseeable future as it is more likely than not that some or all of those deferred tax assets may not be realized based on our history of losses.

Results of Operations

The following tables summarize our unaudited condensed consolidated statements of operations data for the periods presented. The period-to-period comparison of results is not necessarily indicative of results for future periods.

	Three Months Ended April 30,	
	2026	2025
	(in thousands)	
Revenue		
Subscription	\$ 374,153	\$ 265,661
Other	12,915	12,820
Total revenue	387,068	278,481
Cost of revenue		
Subscription ⁽¹⁾	66,723	51,912
Other ⁽¹⁾	8,562	8,571
Total cost of revenue	75,285	60,483
Gross profit	311,783	217,998
Operating expenses		
Research and development ⁽¹⁾	114,341	81,815
Sales and marketing ⁽¹⁾	193,098	169,993
General and administrative ⁽¹⁾	56,978	59,281
Total operating expenses	364,417	311,089
Loss from operations	(52,634)	(93,091)
Interest income	15,898	7,696
Interest expense	(1,070)	(9,813)
Other income (expense), net	590	(5,622)
Loss before income taxes	(37,216)	(100,830)
Income tax expense	4,637	1,274
Net loss	\$ (41,853)	\$ (102,104)
Net loss per share, basic and diluted	\$ (0.21)	\$ (0.53)
Weighted-average shares used in computing net loss per share, basic and diluted	203,668	191,625

(1) Includes stock-based compensation expense as follows:

	Three Months Ended April 30,	
	2026	2025
	(in thousands)	
Cost of revenue		
Subscription	\$ 4,631	\$ 3,968
Other	634	857
Research and development	33,026	19,812
Sales and marketing	16,331	24,144
General and administrative	18,746	24,759
Total stock-based compensation expense	\$ 73,368	\$ 73,540

[Table of Contents](#)

The following table sets forth our unaudited condensed consolidated statements of operations data expressed as a percentage of revenue for the periods indicated:

	Three Months Ended April 30,	
	2026	2025
Revenue		
Subscription	97 %	95 %
Other	3	5
Total revenue	100	100
Cost of revenue		
Subscription	17	19
Other	2	3
Total cost of revenue	19	22
Gross profit	81	78
Operating expenses		
Research and development	30	29
Sales and marketing	50	61
General and administrative	15	21
Total operating expenses	95	111
Loss from operations	(14)	(33)
Interest income	4	3
Interest expense	—	(4)
Other income (expense), net	—	(2)
Loss before income taxes	(10)	(36)
Income tax expense	1	1
Net loss	(11)%	(37)%

Comparison of the Three Months Ended April 30, 2026 and 2025

Revenue

	Three Months Ended April 30,		\$ Change	% Change
	2026	2025 (dollars in thousands)		
Revenue				
Subscription	\$ 374,153	\$ 265,661	\$ 108,492	41 %
Other	12,915	12,820	95	1 %
Total revenue	\$ 387,068	\$ 278,481	\$ 108,587	39 %

Growth in subscription revenue for the three months ended April 30, 2026 was driven by growth in Subscription ARR and some benefits as customers exercised or forfeited their Subscription Credits. For the three months ended April 30, 2026, non-recurring revenue related to material rights associated with Subscription Credits accounted for approximately \$8.5 million of subscription revenue. We expect our subscription revenue to continue to benefit from customers exercising or forfeiting their Subscription Credits through fiscal 2027, although we expect the benefits to significantly decline sequentially.

Our Subscription ARR grew from \$1.18 billion as of April 30, 2025 to \$1.57 billion as of April 30, 2026, representing a 32% increase. Of the increase in Subscription ARR, approximately 0.4 percentage points are a result of transitioning our existing maintenance customers to our subscription editions. A further indication of our ability to expand revenue from existing customers is through our average subscription dollar-based net retention rate which was approximately 120% as of April 30, 2026. We had 2,946 customers with \$100,000 or more in Subscription ARR as of April 30, 2026, increasing from 2,381 as of April 30, 2025.

Other revenue, which consists primarily of sales of perpetual licenses of our legacy CDM product, Rubrik-branded Appliances and professional services, was relatively flat for the three months ended April 30, 2026. Other revenue represented 3% and 5% of total revenue for the three months ended April 30, 2026 and 2025, respectively. The transition of existing maintenance customers adopting RSC subscription offerings was largely completed in fiscal 2026. We expect our other revenue as a percentage of total revenue to continue to decrease.

Cost of Revenue

	Three Months Ended April 30,		\$ Change	% Change
	2026	2025		
	(dollars in thousands)			
Cost of revenue				
Subscription	\$ 66,723	\$ 51,912	\$ 14,811	29 %
Other	8,562	8,571	(9)	— %
Total cost of revenue	<u>\$ 75,285</u>	<u>\$ 60,483</u>	<u>\$ 14,802</u>	24 %

Cost of subscription revenue increased for the three months ended April 30, 2026 primarily driven by an increase of \$8.5 million in hosting costs due to the launch and adoption of more SaaS offerings by our customers, an increase of \$2.7 million from growth in our customer support organization, an increase of \$1.8 million of amortization of acquired technology and an increase of \$1.5 million of amortization of capitalized internal-use software.

Gross Profit and Gross Margin

	Three Months Ended April 30,		\$ Change	% Change
	2026	2025		
	(dollars in thousands)			
Gross profit				
Subscription	\$ 307,430	\$ 213,749	\$ 93,681	44 %
Other	4,353	4,249	104	2 %
Total gross profit	<u>\$ 311,783</u>	<u>\$ 217,998</u>	<u>\$ 93,785</u>	43 %

	Three Months Ended April 30,		\$ Change	% Change
	2026	2025		
Gross margin				
Subscription			82 %	80 %
Other			34 %	33 %
Total gross margin			81 %	78 %

Subscription gross margin increased for the three months ended April 30, 2026, primarily driven by economies of scale as our subscription revenue base expanded faster than our associated cost of revenue.

Operating Expenses

Research and Development

	Three Months Ended April 30,		\$ Change	% Change
	2026	2025		
	(dollars in thousands)			
Research and development	\$ 114,341	\$ 81,815	\$ 32,526	40 %

Research and development expenses increased for the three months ended April 30, 2026 primarily due to an increase of \$19.9 million in employee related costs driven by an increase in headcount, of which \$13.2 million is an increase in stock-based compensation expense. In addition, hosting and software expenses increased by \$9.8 million.

Sales and Marketing

	Three Months Ended April 30,		\$ Change	% Change
	2026	2025		
	(dollars in thousands)			
Sales and marketing	\$ 193,098	\$ 169,993	\$ 23,105	14 %

Sales and marketing expenses increased for the three months ended April 30, 2026 primarily due to an increase of \$11.5 million in marketing expense as a result of advertising costs, marketing events and related costs to promote and expand our market presence, and an increase of \$7.0 million in employee related costs driven by an increase in headcount.

General and Administrative

	Three Months Ended April 30,		\$ Change	% Change
	2026	2025		
	(dollars in thousands)			
General and administrative	\$ 56,978	\$ 59,281	\$ (2,303)	(4)%

General and administrative expenses decreased for the three months ended April 30, 2026 primarily driven by a decrease of \$6.0 million in stock-based compensation expense mainly related to performance-based equity awards. The decrease is offset by an increase of \$1.5 million in employee related costs driven by an increase in headcount and an increase of \$1.3 million in third-party consulting and professional services expenses.

Other Non-Operating Income (Expense)

	Three Months Ended April 30,		\$ Change	% Change
	2026	2025		
	(dollars in thousands)			
Interest income	\$ 15,898	\$ 7,696	\$ 8,202	107 %
Interest expense	(1,070)	(9,813)	8,743	(89)%
Other income (expense), net	590	(5,622)	6,212	(110)%

Interest income increased for the three months ended April 30, 2026 due to higher cash, cash equivalents, and investment balances.

Interest expense decreased for the three months ended April 30, 2026 as our 2023 Amended Credit Facility with Goldman Sachs BDC, Inc. and the other lenders party thereto was fully repaid in June 2025.

Other income (expense), net includes foreign exchange gains and losses and fluctuations are driven by the strengthening or weakening of the US dollar against foreign currencies on our foreign-denominated intercompany payables.

Income Tax Expense

	Three Months Ended April 30,		\$ Change	% Change
	2026	2025		
	(dollars in thousands)			
Income tax expense	\$ 4,637	\$ 1,274	\$ 3,363	264 %

Our income tax expense increased for the three months ended April 30, 2026 due to increased profits in our foreign subsidiaries.

Our effective tax rate may fluctuate significantly and could be adversely affected to the extent that earnings are lower than anticipated in countries that have lower statutory tax rates and higher than anticipated in countries that have higher statutory tax rates. In addition, tax authorities may challenge our transfer pricing policies, resulting in a higher effective tax rate.

Liquidity and Capital Resources

As of April 30, 2026, we had cash, cash equivalents, and short-term investments of \$1.75 billion. Our cash equivalents and investments primarily consist of money market funds, certificate of deposit, U.S. treasuries, commercial paper, corporate bonds, and U.S. government agencies securities. We have generated significant operating losses from our operations as reflected in our accumulated deficit of \$3.23 billion as of April 30, 2026. We expect to continue to incur operating losses, and our operating cash flows may fluctuate between positive and negative amounts for the foreseeable future. As a result, we may require additional capital resources to execute strategic initiatives to grow our business.

Our primary sources of cash are payments received from our customers as well as net proceeds from the issuance of our Convertible Notes. Our primary uses of cash include personnel-related expenses, third-party cloud infrastructure expenses, sales and marketing expenses, overhead costs, and strategic acquisitions we may make from time to time.

Our billings grow with new business growth. The majority of our billings are driven by invoicing our customers for multi-year commitments. However, this may evolve as customers have opted to, and may continue to opt to, pay us on an annual, monthly or consumption basis based on products purchased due to the growth in our SaaS and Cloud product offerings. In addition, our billings are subject to seasonality, with billings in the fourth quarter being substantially higher than in the other three quarters.

We believe that our existing cash, cash equivalents and short-term investments will be sufficient to fund our operating and capital needs for at least the next 12 months.

Our longer-term future capital requirements will depend on many factors, including our subscription growth rate, subscription renewal activity, including the timing and the amount of cash received from customers, the expansion of sales and marketing activities, the timing and extent of spending to support development efforts, the introduction of new and enhanced products, and the continuing market adoption of our platform. We believe we will meet longer-term expected future cash requirements and obligations through a combination of cash flows from operating activities, available cash and short-term investment balances, and potential future debt or equity financings. We may in the future enter into arrangements to acquire or invest in complementary businesses, services, and technologies, including intellectual property rights. We continue to assess our capital structure and evaluate the merits of deploying available cash. We may be required to seek additional equity or debt financing. In the event that additional financing is required from outside sources, we may not be able to raise it on terms acceptable to us or at all. If we are unable to raise additional capital when desired, or if we cannot expand our operations or otherwise capitalize on our business opportunities because we lack sufficient capital, our business, financial condition, and operating results would be adversely affected.

Convertible Senior Notes

In June 2025, we completed a private offering to qualified institutional buyers of \$1.15 billion aggregate principal amount of 0.00% convertible senior notes due 2030. The Convertible Notes are general unsecured obligations of the Company and will mature on June 15, 2030, unless earlier converted, redeemed or repurchased. Net proceeds from the issuance of the Convertible Notes were approximately \$1.13 billion. The outstanding principal of the Convertible Notes was \$1.15 billion as of April 30, 2026.

In connection with the Convertible Notes, we entered into privately negotiated capped call transactions with certain affiliates of certain initial purchasers of the Convertible Notes and other financial institutions (the “Capped Calls”) for a cost of \$88.6 million. The Capped Calls are expected generally to reduce the potential dilution to our Class A common stock upon any conversion of the Convertible Notes and/or offset any cash payments we are required to make in excess of the principal amount of converted Convertible Notes, as the case may be, with such reduction and/or offset subject to a cap based on the cap price initially equal to \$175.10 per share. We used a portion of the net proceeds from the Convertible Notes to pay the \$88.6 million cost of the Capped Calls and repaid the outstanding balance of \$327.9 million under our prior credit facility. We expect to use the remaining net proceeds from the Convertible Notes for general corporate purposes, which may include acquisitions or strategic investments in complementary businesses or technologies, working capital, operating expenses and capital expenditures.

The following table summarizes our cash flows for the periods presented:

	Three Months Ended April 30,	
	2026	2025
	(in thousands)	
Net cash provided by operating activities	\$ 81,689	\$ 39,655
Net cash (used in) provided by investing activities	\$ (36,183)	\$ 34,165
Net cash provided by financing activities	\$ 17,215	\$ 15,341

Operating Activities

Our largest source of operating cash is payments received from our customers. We typically invoice our customers in advance for multi-year contracts. Therefore, a substantial source of our cash is from such prepayments, which are included on our unaudited condensed consolidated balance sheets in deferred revenue. We generally experience seasonality based on when we enter into agreements with our customers. Given the seasonality in our business, the operating cash flow benefit from increased collections from our customers generally occurs in the subsequent quarter after billing. We expect seasonality, timing of billings, billings terms, and collections from our customers to have a material impact on our cash flow from operating activities from period to period. Our primary uses of cash in operating activities are for employee compensation and related expenses, sales commissions, fees for third-party professional services, colocation and hosting costs, marketing programs, and prepayments of other spend, including hosting prepayments. Our cash flow from operating activities may fluctuate due to the timing of cash payments received from our customers and payments relative to expenses.

For the three months ended April 30, 2026, net cash provided by operating activities of \$81.7 million resulted primarily from a net loss of \$41.9 million, partially offset by \$73.4 million of stock-based compensation, \$29.3 million of amortization of deferred commissions, \$12.1 million for depreciation and amortization, and \$6.4 million of net cash inflow from changes in operating assets and liabilities. The net cash inflow from changes in operating assets and liabilities was primarily the result of a \$57.4 million decrease in accounts receivable, a \$43.1 million increase in deferred revenue from increased billings, and a \$13.8 million decrease in prepaid expenses and

other assets. The cash inflow was partially offset by a \$80.4 million decrease in accrued expenses and other liabilities, and a \$26.6 million increase in deferred commissions.

For the three months ended April 30, 2025, net cash provided by operating activities of \$39.7 million resulted primarily from a net loss of \$102.1 million, partially offset by \$73.5 million of stock-based compensation, \$24.8 million of amortization of deferred commissions, \$8.1 million for depreciation and amortization, and \$35.1 million of net cash inflow from changes in operating assets and liabilities. The net cash inflow from changes in operating assets and liabilities was primarily the result of a \$89.7 million increase in deferred revenue from increased billings and a \$12.0 million decrease in accounts receivable. The cash inflow was partially offset by a \$36.8 million decrease in accrued expenses and other current liabilities, a \$21.4 million increase in deferred commissions, and a \$7.8 million increase in prepaid expense and other assets.

Investing Activities

For the three months ended April 30, 2026, net cash used in investing activities of \$36.2 million resulted from \$292.0 million in purchases of investments, \$3.8 million in capitalized internal-use software, and \$4.3 million in purchases of property and equipment, partially offset by \$263.9 million in proceeds from maturities of investments.

For the three months ended April 30, 2025, net cash provided by investing activities of \$34.2 million resulted from \$162.6 million in proceeds from maturities and sales of investments, partially offset by \$120.2 million in purchases of investments, \$3.5 million in capitalized internal-use software, and \$2.8 million in purchases of property and equipment.

Financing Activities

For the three months ended April 30, 2026, net cash provided by financing activities of \$17.2 million resulted primarily from \$16.6 million in proceeds from issuance of common stock under employee stock purchase plan and \$0.6 million from the exercise of stock options.

For the three months ended April 30, 2025, net cash provided by financing activities of \$15.3 million resulted from \$13.5 million in proceeds from issuance of common stock under employee stock purchase plan and \$1.8 million from the exercise of stock options.

Material Cash Requirements

Our material cash requirements primarily consist of operating lease commitments for our offices and data centers, non-cancelable purchase commitments related to third-party cloud hosting services, and long-term debt. Except as already disclosed in Note 7, Debt and Note 8, Commitments and Contingencies in our unaudited condensed consolidated financial statements included elsewhere in this Quarterly Report on Form 10-Q, there has been no other material change in our material cash requirements other than in the ordinary course of business since our fiscal year ended January 31, 2026. See our Annual Report for additional information regarding our contractual obligations.

Critical Accounting Policies and Estimates

Refer to Part II, Item 7, “Critical Accounting Policies and Estimates” of our Annual Report on Form 10-K for the fiscal year ended January 31, 2026. There have been no material changes to our Critical Accounting Policies and Estimates.

Recently Issued Accounting Pronouncements

See Note 2, Basis of Presentation and Summary of Significant Accounting Policies, in the notes to our unaudited condensed consolidated financial statements included in Part I, Item I of this Quarterly Report on Form 10-Q for a discussion of recent accounting pronouncements.

Item 3. Quantitative and Qualitative Disclosures About Market Risk

We have operations in the United States and internationally, and we are exposed to market risk in the ordinary course of our business.

Interest Rate Risk

As of April 30, 2026, we had cash, cash equivalents, and short-term investments of \$1.75 billion and restricted cash of \$16.6 million. Our cash, cash equivalents, and short-term investments are held for working capital purposes. We do not enter into investments for trading or speculative purposes. Our investments are exposed to market risk due to fluctuations in interest rates, which may affect our interest income. A hypothetical 1% increase or decrease in interest rates would not have a material effect on the fair market value of our portfolio.

In June 2025, we issued \$1.15 billion aggregate principal amount of Convertible Notes in a private offering to qualified institutional buyers. The fair value of the Convertible Notes is subject to market risk and other factors due to the conversion feature. The fair value of the Convertible Notes generally increases as our Class A common stock price increases, and generally decreases as our Class A common stock price declines. The market value changes affect the fair value of the Convertible Notes, but do not impact our financial position, cash flows or results of operations due to the fixed nature of the debt obligation.

Foreign Currency Risk

Our reporting currency is the U.S. dollar and the functional currency for all of our foreign subsidiaries are the respective local currencies. All of our sales contracts are denominated in U.S. dollars. A portion of our operating expenses are incurred outside of the United States, denominated in foreign currencies, and subject to fluctuations due to changes in foreign currency exchange rates. Our unaudited condensed consolidated results of operations and cash flows are, therefore, subject to fluctuations due to changes in foreign currency exchange rates and may be adversely affected in the future due to changes in foreign exchange rates. To date, we have not entered into any hedging arrangements with respect to foreign currency risk or other derivative financial instruments, although we may choose to do so in the future. We do not believe a 10% increase or decrease in the relative value of the U.S. dollar would have a material impact on our results of operations.

Item 4. Controls and Procedures

Evaluation of Disclosure Controls and Procedures

Our management, with the participation of our Chief Executive Officer and Chief Financial Officer, has evaluated the effectiveness of our disclosure controls and procedures as of the end of the period covered by this Quarterly Report on Form 10-Q. The term “disclosure controls and procedures,” as defined in Rules 13a-15(e) and 15d-15(e) under the Securities Exchange Act of 1934, as amended (the “Exchange Act”), means controls and other procedures of a company that are designed to ensure that information required to be disclosed by a company in the reports that it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the SEC’s rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to provide reasonable assurance that information required to be disclosed by a company in the reports that it files or submits under the Exchange Act is accumulated and communicated to the company’s management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure. Based on such evaluation, our Chief Executive Officer and Chief Financial Officer concluded that, as of the end of the period covered by this Quarterly Report on Form 10-Q, our disclosure controls and procedures were effective at the reasonable assurance level.

Changes in Internal Control over Financial Reporting

There were no changes in our internal control over financial reporting identified in connection with the evaluation required by Rule 13a-15(d) and 15d-15(d) of the Exchange Act that occurred during the period covered by this Quarterly Report on Form 10-Q that have materially affected, or are reasonably likely to materially affect, our internal control over financial reporting.

Inherent Limitations on Effectiveness of Controls

Our management, including our Chief Executive Officer and Chief Financial Officer, believes that our disclosure controls and procedures and internal control over financial reporting are designed to provide reasonable assurance of achieving their objectives and are effective at the reasonable assurance level. However, management does not expect that our disclosure controls and procedures or our internal control over financial reporting will prevent or detect all errors and all fraud. A control system, no matter how well conceived and operated, can provide only reasonable, not absolute, assurance that the objectives of the control system are met. Because of the inherent limitations in all control systems, no evaluation of controls can provide absolute assurance that all control issues and instances of fraud, if any, within the company have been detected. The design of any system of controls also is based in part upon certain assumptions about the likelihood of future events, and there can be no assurance that any design will succeed in achieving its stated goals under all potential future conditions. Over time, controls may become inadequate because of changes in conditions, or the degree of compliance with the policies or procedures may deteriorate. Because of the inherent limitations in a cost-effective control system, misstatements due to error or fraud may occur and not be detected.

PART II. OTHER INFORMATION

Item 1. Legal Proceedings

From time to time, we are involved in various legal proceedings arising from activities in the normal course of business. We are not presently a party to any litigation the outcome of which, we believe, if determined adversely to us, would individually or taken together have a material adverse effect on our business, financial condition, results of operations, and cash flows. Defending any legal proceedings is costly and can impose a significant burden on management and employees. The results of any current or future litigation cannot be predicted with certainty, and regardless of the outcome, litigation can have an adverse impact on us because of defense and settlement costs, diversion of management resources, and other factors.

Item 1A. Risk Factors

Investing in our Class A common stock involves various risks, including those described below. You should consider and read carefully all of the risks and uncertainties described below, together with all of the other information contained in this Quarterly Report on Form 10-Q, including the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations" and our unaudited condensed consolidated financial statements and related notes, before making an investment decision. The risks described below are not the only ones we face. The occurrence of any of the following risks or additional risks and uncertainties not presently known to us or that we currently believe to be immaterial could materially and adversely affect our business, financial condition, or results of operations. In such case, the trading price of our Class A common stock could decline, and you may lose some or all of your original investment.

Risks Related to Our Business

Our recent rapid growth may not be indicative of our future growth. Our rapid growth also makes it difficult to evaluate our future prospects.

Our revenue was \$387.1 million and \$278.5 million for the three months ended April 30, 2026 and 2025, respectively. You should not rely on the revenue growth of any prior period as an indication of our future performance. Even if our revenue continues to increase, we expect that our revenue growth rate will fluctuate in the future as a result of a variety of factors. While we have largely completed both the sales of Rubrik-branded Appliances transitioning from us to our contract manufacturers in fiscal 2025 and the transition for new and existing customers to sales of RSC in fiscal 2026, we expect our subscription revenue to continue to benefit from customers exercising or forfeiting their Subscription Credits (which are customer options that are accounted for as material rights) through fiscal 2027, although we expect the benefits to significantly reduce sequentially. These business transitions cause fluctuations to our total revenue growth and limit the comparability of our revenue with past performance.

Overall growth of our revenue also depends on a number of factors, including our ability to:

- expand the features and functionality of our data security products as well as increase the amount of data sources protected across enterprise, cloud, SaaS, unstructured data, and identity providers;
- securely deploy generative AI while delivering exceptional accuracy and efficiency using agentic applications;
- extend our product leadership to expand our addressable market;
- differentiate our products from those offered by others;
- successfully develop a substantial sales pipeline for our products;
- hire sufficient sales personnel to support our growth and reduce the time for such personnel to achieve desired productivity levels;
- attract new customers and expand sales to our existing customers, including by effectively marketing and pricing our data security products and successfully transitioning existing customers to RSC;
- increase awareness of our brand on a global basis as a data security company to successfully compete with other companies;
- provide our customers with support that meets their needs;
- effectively leverage and expand our partner ecosystem;
- navigate macroeconomic headwinds, including those related to inflation, tariffs, and geopolitical conditions, as well as supply chain constraints affecting the availability and pricing of compatible commodity servers needed to deploy our solutions;
- protect against security incidents;
- successfully protect our intellectual property in the United States and other jurisdictions; and
- expand to new international markets and grow within existing markets.

We may not successfully accomplish any of these objectives, and as a result, it is difficult for us to forecast our future results of operations. If the assumptions that we use to plan our business are incorrect or if we are unable to maintain consistent revenue or revenue growth, our stock price could be volatile and we may not be able to achieve and maintain profitability.

In addition, we expect to continue to expend substantial financial and other resources on:

- expansion and enablement of our sales, services, and marketing organizations to increase brand awareness and drive adoption of our solutions;
- product development, including investments in our product development team and the development of new products, new features, and functionality for our platform and products;
- our cloud infrastructure technology, including systems architecture, scalability, availability, performance, and security;
- our use and development of AI technologies and tools;
- our partner ecosystem;
- international expansion;
- acquisitions or strategic investments;
- our information security program; and
- general administration, including increased legal, human resources, and accounting expenses associated with being a public company.

These investments may not result in increased revenue for our business. If we are unable to maintain or increase our revenue at a rate sufficient to offset the expected increase in our costs, our business, financial condition, and results of operations will be harmed, and we may not be able to achieve or maintain profitability. Additionally, we may encounter unforeseen operating expenses, difficulties, complications, delays, decreased revenue growth associated with general macroeconomic and market conditions, volatility, or disruptions (including the effect of those events on our customers) and other unknown factors that may result in losses in future periods. If our revenue does not meet our expectations in future periods, our business, financial condition, and results of operations may be harmed.

If the market for data security and AI solutions does not grow, our ability to grow our business and our results of operations may be adversely affected.

We believe our future success will depend in large part on the growth, if any, in the market for data security and AI solutions. Traditionally, the cybersecurity industry has been focused on securing information technology infrastructure to prevent, detect, and investigate cyberattacks. Our platform brings a new approach to cybersecurity, which involves protecting our customers' data across enterprise, cloud, SaaS, unstructured data, and identity providers, observing the data itself to proactively identify emergent threats, remediating data security threats, and recovering protected data following a cybersecurity event, as well as helping customers manage risks associated with AI agents. The market for data security and AI solutions, such as our platform and data security products, is at an early stage and rapidly evolving. As such, it is difficult to predict this market's potential growth, if any, customer adoption and retention rates, customer demand for data security platforms, or the success of competitive products. In the past, customer adoption of our platform and data security products has been driven by the need for data resilience due to increasing ransomware activity. We do not know whether the trends of increasing ransomware activity, or of increasing adoption of our platform and data security products such as ours that we have experienced in the past, will continue in the future. Any expansion in this market depends on a number of factors, including the cost, performance, and perceived value associated with our platform and data security products and similar solutions of our competitors, including preference to manage security with existing infrastructure security tools alone, rather than investing in a platform based solution. The markets for some of our solutions are new, unproven, and evolving, and our future success depends on growth and expansion of these markets. If our platform and data security products do not achieve widespread adoption or there is a reduction in demand for our platform and data security products due to a lack of customer acceptance, technological challenges, competing products or solutions, privacy concerns, decreases in corporate spending, weakening economic conditions, or otherwise, it could result in early terminations, reduced customer retention rates, or decreased revenue, any of which would adversely affect our business, financial condition, and results of operations. You should consider our business and growth prospects in light of the risks and difficulties we encounter in this new and evolving market.

We have a limited operating history, particularly with respect to our offerings of RSC and RAC, which makes it difficult to forecast our future results of operations.

Although we were founded in December 2013, we only began offering our products and services in the fiscal year ended January 31, 2016, and we began offering RSC as a cloud native SaaS solution in fiscal 2023 and introduced the RAC suite in fiscal 2026. As a result of our limited operating history, our ability to accurately forecast our future results of operations is limited and subject to a number

of uncertainties, including our ability to plan for and forecast future growth. Our historical revenue growth should not be considered indicative of our future performance. In future periods, our revenue growth may fluctuate, slow or decline due to a number of factors, including changes in product mix. While we have largely completed both the transition of sales of Rubrik-branded Appliances from us to our contract manufacturers in fiscal 2025 and the transition for new and existing customers to sales of RSC in fiscal 2026, we expect our subscription revenue to continue to benefit from customers exercising or forfeiting their Subscription Credits (which are customer options that are accounted for as material rights) through fiscal 2027, although we expect the benefits to significantly reduce sequentially. These business transitions cause fluctuations to our total revenue growth and limit the comparability of our revenue with past performance.

In addition, we operate in a new market for data security and AI solutions, and as such we have encountered, and will continue to encounter, risks and uncertainties frequently experienced by growing companies in new and rapidly changing markets, such as the risks and uncertainties described throughout this section. Further, our business and growth strategies are also dependent on continued development, and implementation and integration of our AI offerings and initiatives, including RAC, which is designed to accelerate enterprise AI agent deployments. While we have invested significantly in our AI offerings and initiatives and intend to continue doing so in the future, AI technology is expected to continue to rapidly advance. We may not be successful in obtaining and maintaining market acceptance of our AI offerings and initiatives, including RAC, particularly as competitive technologies and solutions are introduced. Any of these outcomes could harm our business, results of operations, and financial condition.

Moreover, in future periods, our revenue growth could slow or decline due to slowing demand for our platform or data security products, increasing competition, decreased productivity of our sales and marketing organization, failure to retain existing customers or expand existing subscriptions, changing technology, a decrease in the growth of our overall market, evolving macroeconomic conditions, such as high inflation and recessionary environments, or our failure, for any reason, to continue to take advantage of growth opportunities. If our assumptions regarding these risks and uncertainties and our future revenue growth are incorrect or change, or if we do not address these risks successfully, our financial condition and results of operations could differ materially from our expectations, and our business could suffer.

If we are unable to attract new customers, our future results of operations could be harmed.

To expand our customer base, we need to convince organizations to allocate a portion of their discretionary budgets to purchase our platform and products. Our sales efforts often involve educating organizations about the uses and benefits of our data security and AI solutions. We may have difficulty convincing organizations of the value of adopting our solutions. Even if we are successful in convincing organizations that a platform like ours is critical to secure their data, they may not decide to purchase our solutions for a variety of reasons, some of which are out of our control. For example, any deterioration in general economic conditions has in the past caused, and may in the future cause, our current and prospective customers to delay or cut their overall security and IT operations spending. Macroeconomic concerns, customer financial difficulties, and constrained spending on security and IT operations may result in decreased revenue and adversely affect our financial condition and results of operations. In particular, uncertainty related to geopolitical conditions, supply chain issues, and trade tensions may impact customer adoption and use of our offerings and revenue from sales of our products and services. Additionally, if the incidence of cyberattacks were to decline, or enterprises or governments perceive that the general level of cyberattacks has declined, our ability to attract new customers could be adversely affected. We may face additional difficulties in attracting organizations that use legacy data management products to purchase our data security products if they believe that these legacy products are more cost-effective or provide a level of IT security that is sufficient to meet their needs. Furthermore, the use of our data security products to manage data security, movement, and restoration across data centers is relatively new, and if we are unable to convince organizations of the benefits of our products, then our business, financial condition, and results of operations could be adversely impacted.

We have a history of operating losses and may not achieve or sustain profitability in the future.

We have experienced net losses in each period since inception. We generated net losses of \$(41.9) million and \$(102.1) million for the three months ended April 30, 2026 and 2025, respectively. As of April 30, 2026 and January 31, 2026, we had an accumulated deficit of \$(3.23) billion and \$(3.19) billion, respectively. While we have experienced rapid revenue growth in recent periods, we are not certain whether or when we will obtain a high enough volume of sales to achieve or maintain profitability in the future. In particular, as we expand the availability of our platform, increase our ability to secure data across multiple different sources, and add more capabilities, our ability to achieve and maintain profitability will be highly dependent on our ability to successfully market our platform and data security products to new and existing customers. We also expect our costs and expenses to increase in future periods, which could negatively affect our future results of operations if our revenue does not increase. In particular, we intend to continue to expend significant funds to further develop our offerings, including by introducing new features and functionality and securing additional applications, and to expand our sales, marketing, and services teams to drive new customer adoption, expand the use of our data security products by existing customers, support international expansion, and implement additional systems and processes to

effectively scale operations. We will also face increased compliance costs associated with growth, the planned expansion of our customer base and pipeline, international expansion, and being a public company. In addition, our data security and AI solutions operate on a public cloud infrastructure provided by third-party vendors, including Google Cloud (“GCP”), Microsoft Azure (“Azure”), and Amazon Web Services (“AWS”), and our costs and gross margins are significantly influenced by the prices we are able to negotiate with these public cloud providers. To the extent we are able to drive adoption of our platform and data security products, we may incur increased costs related to our public cloud contracts, which would negatively impact our gross margins. Our efforts to grow our business may be costlier than we expect, or the rate of our growth in revenue may be slower than we expect, and we may not be able to increase our revenue enough to offset our increased operating expenses. In addition, our efforts and investments to implement systems and processes to scale operations may not be sufficient or may not be appropriately executed. As a result, we may incur significant losses in the future for a number of reasons, including the other risks described herein, unforeseen expenses, difficulties, complications, or delays, and other unknown events. If we are unable to achieve and sustain profitability, the value of our business and Class A common stock may significantly decrease.

Furthermore, we have historically sold our products to customers as perpetual licenses with associated maintenance contracts or as subscription term-based licenses with associated support, and with respect to the latter, we recognized a portion of the revenue upfront at the time we transferred control of the subscription term-based license to the customer and deferred the remainder. We have substantially completed our transition to offering our platform primarily through SaaS subscriptions, and a significant majority of our new and existing customers have adopted RSC on a SaaS subscription basis. As of the end of fiscal 2026, SaaS subscriptions represented a majority of our total revenue. We have also largely completed the transition of sales of Rubrik-branded Appliances from us to our contract manufacturers in fiscal 2025. We expect our subscription revenue to continue to benefit from customers exercising or forfeiting their Subscription Credits (which are customer options that are accounted for as material rights) through fiscal 2027, although we expect the benefits to significantly reduce sequentially. These business transitions may continue to cause fluctuations to our total revenue growth and limit the comparability of our revenue with past performance. In addition, the stock-based compensation expense related to our RSUs has resulted in and will continue to result in significant increases in our expenses in future periods, which may negatively impact our ability to achieve profitability.

If our customers do not renew their subscriptions for our platform and products or expand their subscriptions to increase the amount of data secured, secure new applications, or include new features or capabilities, our results of operations could be harmed.

In order for us to maintain or improve our results of operations, it is important that our customers renew their subscriptions for our data security solutions, add data security or AI products, and increase the volume of their data protected by our solutions. Our AI solutions, including RAC, are relatively new, and customer adoption and expansion of these solutions may be uncertain. We expand our commercial purchase relationships with our existing customers as they increase the volume of their data protected by our data security solutions and secure additional applications and workloads. Our customers have no obligation to renew their subscription for our data security solutions after the expiration of their contractual subscription period, which is generally three years, and in the normal course of business, some customers have elected not to renew their subscriptions. In addition, customers may elect to shorten the term of their subscription, select a lower subscription edition, or purchase less capacity. Our customer retention and expansion may also decline or fluctuate as a result of a number of factors, including our customers’ satisfaction with our data security solutions, our pricing, customer prioritization of security, our customers’ security and IT operations spending, our customers’ ability to procure Rubrik-branded Appliances or other compatible third-party commodity servers to implement our data security products, mergers and acquisitions involving our customers, industry developments, competition, changing regulatory environments, and macroeconomic uncertainty related to recent global tariffs, the direct and indirect impact of which continues to evolve. Moreover, customers tend to expand their usage of our data security solutions over time as the amount of data they need to protect grows. As a result, strong customer retention over time generally leads to a higher degree of usage of our solutions. Therefore, a decline in customer retention may have a significant impact on our results of operations, including a decline in our average subscription dollar-based net retention rate, which could cause the price of our Class A common stock to decline or fluctuate. If our efforts to maintain and expand our relationships with our existing customers are not successful, our business, financial condition, and results of operations may suffer.

If our solutions fail or do not perform as intended or are perceived to have defects, errors, or vulnerabilities, our brand and reputation will be harmed, which would adversely affect our business and results of operations.

Our solutions are complex and, like all software, have in the past contained and may in the future contain undetected defects, errors, or vulnerabilities. From time to time, we identify certain vulnerabilities in our information systems. While we take steps designed to mitigate the risks associated with known vulnerabilities, there can be no assurance that any vulnerability mitigation measures will be effective. Moreover, we may also experience delays in developing and deploying remedial measures and patches designed to address any identified vulnerabilities. Real or perceived defects, errors, or vulnerabilities in our solutions, the failure of our solutions to secure, observe, and restore our customers’ data, misconfiguration of our solutions, the exploitation of any known or unknown vulnerabilities, or

the failure of customers to deploy our solutions in combination with industry best practices could harm our reputation, result in a loss of, or delay in, market acceptance of our solutions, result in a loss of existing or potential customers, and adversely affect our business, financial condition, and results of operations. We are continuing to evolve the features and functionality of our products through updates and enhancements, and as we do so, we may inadvertently introduce defects, errors, or vulnerabilities that may not be detected until after deployment by our customers. In addition, implementation or use of our solutions that is not correct or as intended may result in adverse consequences such as inadequate performance and disruptions in service. Moreover, if we acquire companies or technologies developed by third parties, difficulties integrating such acquired technologies may result in product flaws or software vulnerabilities.

Additionally, we cannot assure you that our solutions will prevent all data loss or other types of data security incidents, especially in light of the rapidly changing security threat landscape that our solutions seek to address. Due to a variety of both internal and external factors, our solutions could become vulnerable to security incidents (both from intentional attacks and accidental causes) that could cause them to fail to adequately secure or observe data or to restore data in the event of a security incident.

Moreover, our solutions are adopted by, and part of the supply chain of, a large and increasing number of organizations worldwide, our solutions have been and may in the future be subject to continued, persistent research and reconnaissance by threat actors in order to discover and exploit weaknesses in our technology that can be exploited. If our solutions are compromised, a significant number or, in some instances, all of our customers and their data could be adversely affected. The potential liability and associated consequences we could suffer as a result of such a large-scale event could be catastrophic and result in irreparable harm. Since our business is focused on providing data security services to our customers, an actual or perceived security incident affecting our solutions would be especially detrimental to our reputation and our business.

Because we can access customer data in certain limited circumstances, such as when providing customer support, and such customer data in some cases may contain personal data or confidential information, a security compromise, or an accidental or intentional misconfiguration or malfunction of our platform, could result in personal data and other confidential information being compromised. We and our service providers have been subject to cyberattacks that have occurred in the past and may occur in the future, and our customers or other organizations may lose trust in solutions such as ours.

Organizations are increasingly subject to a wide variety of cyberattacks on their networks, systems, and data. If any of our customers experience a cyberattack while using our solutions and are unable to secure, observe, or restore their data, such customers could discontinue use of our solutions, regardless of whether our solutions were adequately deployed, configured, or used to protect the data in the customer's environment. Real or perceived security incidents involving our customers' networks could cause disruption or damage to their networks or other negative consequences and could result in negative publicity to us, damage to our reputation, and other customer relations issues, any of which may adversely affect our revenue and results of operations.

In addition, errors in our solutions could cause system failures, loss of data, or other adverse effects for our customers, which may result in the assertion of warranty and other claims for substantial damages against us. The potential liability and associated consequences we could suffer as a result of such an incident could be catastrophic and cause irreparable harm to our reputation and results of operations. Although our agreements with our customers typically contain provisions that are intended to limit our exposure to such claims, it is possible that these provisions may not be effective or enforceable under the laws of some jurisdictions. While we seek to insure against these types of claims, our insurance policies may not adequately limit our exposure. These claims, even if unsuccessful, could be costly and time consuming to defend and could harm our business, financial condition, results of operations, and cash flows.

Our information technology systems or data, or those of third parties with whom we work, have in the past been, and may in the future be, compromised, which may cause us to experience significant adverse consequences, including but not limited to regulatory investigations or actions, litigation, fines and penalties, disruptions of our business operations, reputational harm, loss of revenue or profits, loss of customers or sales, and other adverse consequences. As a data security company, we have been and may in the future be specifically targeted by various threat actors who try to compromise our information technology systems or data.

As a SaaS provider, the reliability and continuous availability of our platform is critical to our success. In the ordinary course of our business, we or the third parties with whom we work, collect, receive, store, process, generate, use, transfer, disclose, make accessible, protect, secure, dispose of, transmit, share, or otherwise process proprietary, confidential, and other sensitive data, including customer data (such as confidential customer information or customer content that we may store and protect on behalf of customers), which may include data about individuals, including various data categories and elements associated with an individual, intellectual property, and trade secrets (collectively, Sensitive Information). We collect such information from individuals located both in the United States and abroad and may store or process such information outside the country in which it was collected.

Organizations, particularly organizations like ours that provide data security solutions, experience and are subject to a wide variety of attacks on their networks, systems, and endpoints, and techniques used to sabotage or to obtain unauthorized access to networks in which data is stored or through which data is transmitted change frequently. For example, we have experienced cyber incidents in the past that involved unauthorized access to certain of our systems, but did not result in access to data that we secure on behalf of customers or access to our internal code or disruption to our business or financial systems or to other operations. However, there can be no guarantee that any attack in the future will have a similarly minimal impact, should one occur.

Cyberattacks, malicious internet-based activity, online and offline fraud, and other similar activities threaten the confidentiality, integrity, and availability of our Sensitive Information and information technology systems, and those of the third parties with whom we work. Such threats are prevalent, continuing to rise, increasingly difficult to detect, and come from a variety of sources, including traditional computer “hackers,” threat actors, “hacktivists,” organized criminal threat actors, personnel (such as through theft, misuse, or accidental disclosure), sophisticated nation states, and nation-state-supported actors. Some actors now engage in and are expected to continue to engage in cyberattacks, including without limitation nation-state actors for geopolitical reasons and in conjunction with military conflicts and defense activities. During times of war and other major conflicts, we and the third parties with whom we work, and our customers may be vulnerable to a heightened risk of these attacks, including retaliatory cyberattacks, that could materially disrupt our systems and operations, supply chain, and ability to produce, sell, and distribute our solutions. We and the third parties with whom we work are subject to a variety of evolving threats, including but not limited to social-engineering attacks (including through phishing attacks), malicious code (such as viruses and worms), computer generated or altered fraudulent content (i.e., “deep fakes,” which may be increasingly difficult to identify), malware (including as a result of advanced persistent threat intrusions), denial-of-service attacks, credential stuffing attacks, credential harvesting, personnel misconduct or error, other inadvertent compromises of our systems and data (including those arising from process, coding, or human error), ransomware attacks, supply-chain attacks, software bugs, server malfunctions, software or commodity appliance failures, loss of data or other information technology assets, adware, telecommunications failures, attacks enhanced or facilitated by AI, and other similar threats.

In particular, severe ransomware attacks are becoming increasingly prevalent and can lead to significant interruptions in our operations, loss of sensitive information and income, reputational harm, and diversion of funds. Extortion payments may alleviate the negative impact of a ransomware attack, but we may be unwilling or unable to make such payments due to, for example, applicable laws or regulations prohibiting such payments. Given our data security solutions’ capabilities and marketing and promotional programs related to ransomware recovery, we face heightened risk of being targeted by bad actors.

Moreover, future or past business transactions (such as acquisitions or integrations) could expose us to additional cybersecurity risks and vulnerabilities, as our systems could be negatively affected by vulnerabilities present in acquired or integrated entities’ systems and technologies. Furthermore, we may discover security issues that were not found during due diligence of such acquired or integrated entities, and it may be increasingly difficult to integrate companies into our information technology environment and security program.

We rely on third parties to provide and/or operate critical business systems, process sensitive information, and to help us deliver services to our customers and their end-users. These third parties process customer information in a variety of contexts, including, without limitation, cloud-based infrastructure, data center facilities, encryption and authentication technology, employee email, content delivery to customers, and other functions. For example, our data security solutions are built to be available on the infrastructure of third-party public cloud providers such as GCP, Azure, and AWS. We also rely on other third-party service providers, contract manufacturers, and original equipment manufacturers (OEMs), or collectively with contract manufacturers, Manufacturers, to provide other products or services, or otherwise to assist us with operating our business. While we conduct diligence on these third parties, our ability to monitor these third parties’ information security practices is limited, and these third parties have not had and may not have adequate information security measures in place. In addition, supply-chain attacks have increased in frequency and severity, and we cannot guarantee that third parties’ infrastructure in our supply chain or our third-party partners’ supply chains have not been or will not be compromised.

We take steps designed to detect, mitigate, and remediate vulnerabilities in our information systems (such as our hardware and/or software, including that of third parties with whom we work). However, we have been and may in the future be unable to detect and remediate all such vulnerabilities in our information systems (including our platform and data security products) on a timely basis and there can be no assurance that any vulnerability mitigation measures that we implement will be effective. Further, the process for evaluating potential vulnerabilities and developing and deploying remedial measures and patches designed to address identified vulnerabilities has been and may in the future be lengthy and subject to delays. Vulnerabilities in our information systems have been, and could in the future be, exploited and result in a security incident.

We employ a shared responsibility model where our customers are responsible for using, configuring and otherwise implementing security measures related to our platform, services and products in a manner that meets applicable cybersecurity standards, complies with laws, and addresses their information security risk. As part of this shared responsibility security model, we make certain security

features available to our customers that can be implemented at our customers' discretion or identify security areas or measures for which our customers are responsible. For example, our customers are responsible for adding and enforcing multi-factor authentication to access their accounts. In certain cases where our customers choose not to implement, or incorrectly implement, such features or measures, misuse our services, or otherwise experience their own vulnerabilities, policy violations, credential exposure or security incidents, even if we are not the cause of customer security issue or incident that may result, our customer relationships reputation, and revenue may be adversely impacted. Furthermore, threat actors may also gain access to other networks and systems after a compromise of our networks and systems. For example, threat actors may use an initial compromise of one part of our environment to gain access to other parts of our environment, or leverage a compromise of our networks or systems to gain access to the networks or systems of third parties with whom we work, such as through phishing or supply chain attacks.

Any of the previously identified vulnerabilities or cybersecurity threats have in the past caused and may in the future cause a security incident or other interruption resulting in consequences such as unauthorized, unlawful, or accidental acquisition, modification, destruction, loss, alteration, encryption, disclosure of, or access to our Sensitive Information or our information technology systems, or those of the third parties upon whom we rely. A security incident or other interruption could partially or fully disrupt our ability (and that of third parties upon whom we rely) to provide our platform. Additionally, our business depends upon the appropriate and successful implementation of our platform by our customers. If our customers fail to use our platform according to our specifications or are unwilling or unable to deploy such patches we make available for vulnerabilities effectively or in a timely manner, our customers may suffer a security incident or other interruptions on their own systems or other adverse consequences. Even if such an incident is unrelated to our security practices, it could result in our incurring significant economic and operational costs in investigating, remediating, and implementing additional measures to further protect our customers from their own security issues or vulnerabilities and could result in reputational harm.

Certain data privacy and security obligations may require us to implement and maintain specific security measures or industry standard, reasonable security measures to protect our information technology systems and sensitive information. Additionally, applicable data privacy and security obligations have in the past required us and may in the future require us, or we may voluntarily choose, to notify relevant stakeholders, including affected individuals, customers, regulators, and investors, of security incidents, or to implement other requirements, such as providing credit monitoring. Such disclosures, and compliance with such requirements, are costly, and the disclosure or the failure to comply with such requirements could lead to adverse consequences. Though we have expended, and anticipate continuing to expend, significant resources to try to protect against security incidents by implementing technical, administrative, and physical measures designed to protect the privacy and security of data running through our, and our third parties', systems, it is virtually impossible for us to entirely eliminate the risk of such security incidents or interruptions.

If we (or a third party with whom we work, including our suppliers) experience a security incident or are perceived to have experienced a security incident, which has happened in the past, we may experience adverse consequences such as government enforcement actions (for example, investigations, fines, penalties, audits, and inspections); additional reporting requirements and/or oversight; restrictions on processing data (including data about individuals); litigation (including class claims); indemnification obligations; negative publicity; reputational harm; monetary fund diversions; diversion of management attention; interruptions in our operations (including availability of data); financial loss; and other similar harms. Security incidents and attendant material consequences may prevent or cause customers to stop purchasing our solutions, deter new customers from purchasing our solutions, and negatively impact our ability to grow and operate our business. As a data security company, we could be exposed to additional reputational risks should a security incident occur.

Our contracts may not contain limitations of liability, and even where they do, there can be no assurance that limitations of liability in our contracts are sufficient to protect us from liabilities, damages, or claims related to security incidents, vulnerabilities, or our data privacy and security obligations. We cannot be sure that our insurance coverage will be adequate or sufficient to protect us from or to mitigate liabilities arising out of our privacy and security practices, that such coverage will continue to be available on commercially reasonable terms or at all, or that such coverage will pay future claims.

The limited number of contract manufacturers and original equipment manufacturers that produce commodity servers that are compatible with our solutions are susceptible to supply chain disruptions and have recently experienced shortages of key components for their servers, which may adversely affect our ability to accurately forecast demand for these commodity servers or successfully manage the relationship with such manufacturers, and could negatively impact demand for our offerings, and adversely affect our business and financial results.

A limited number of Manufacturers produce commodity servers that are compatible with our solutions. We do not own or operate any manufacturing facilities and rely on these Manufacturers for such products. These Manufacturers manage the supply chain for these products and, alone or together with us or our distributors and resellers ("Channel Partners"), negotiate component costs. Our reliance on Manufacturers and Channel Partners reduces our control over the assembly process, quality assurance, production costs, and

product supply. If the relationships with Manufacturers are not properly managed or if Manufacturers experience delays, interruptions, or supply-chain disruptions, including due to international conflicts and geopolitical tensions (such as the imposition of new trade restrictions and tariffs due to escalating tensions, hostilities, or trade disputes), health epidemics or pandemics, new trade laws and regulations, capacity constraints, or quality control problems in their operations, the ability for customers to procure compatible commodity servers could be impaired. For example, key components of the commodity servers that are compatible with our solutions have been, and continue to be, adversely affected by global chip shortages and allocation constraints, in part due to elevated industry demand, which in certain cases have resulted in extended lead times and increased server prices. In response to such extended delays or increased costs, we may in the future provide certain commercial accommodations, which could reduce our margins or adversely affect our business if such practices become widespread or prolonged. If such conditions persist or worsen, potential new customers could defer, delay, scale back, or in some cases forego purchases or deployments of our solutions until compatible commodity servers are available or total solution costs decline. Any such disruptions, shortages, or resulting delays may also require us or our Channel Partners to adjust forecasts, reschedule orders, or qualify alternative Manufacturers. If we or our Channel Partners are required to change or qualify a new Manufacturer for any reason, including financial considerations, reduction of manufacturing output made available to us, or the termination of our or our Channel Partners' contract with the Manufacturers, we may lose revenue and incur increased costs to the extent that we are even able to identify and qualify a new Manufacturer. In addition, our contract manufacturers may terminate the agreement with us or our Channel Partners with prior notice for reasons such as failure to perform a material contractual obligation.

A large majority of the customer enterprise data we secure relies upon Rubrik-branded Appliances, which are currently built on servers supplied and designed by Super Micro Computer, Inc. ("Supermicro"). If we are unable to manage our relationship with Supermicro effectively, or if Supermicro continues to suffer delays or disruptions for any reason, including due to the global chip shortage that the broader industry is currently experiencing, any other component allocation constraints, increased manufacturing lead-times, capacity constraints, quality control problems in its manufacturing operations, or international trade disputes, tariffs or other protectionist measures, or fails to meet our requirements for timely delivery, or if Supermicro no longer produces the servers for our Rubrik-branded Appliances, our indirect costs may increase and our end-customer's ability to procure Rubrik-branded Appliances in a timely manner would be impaired to the extent that any alternative commodity servers are available at all. Our agreement with Supermicro does not provide long-term price assurances for certain components used in Rubrik-branded Appliances, and increases in component or server costs could increase the total price customers pay to implement our solutions. While we have largely completed the sales of Rubrik-branded Appliances transitioning from us to our contract manufacturers in fiscal 2025, any such cost increases, including those resulting from chip shortages or allocation constraints, could adversely affect customer demand for our offerings or the timing of purchases and deployments. While customers would have the ability to purchase compatible third-party commodity servers from other OEMs, and we have the ability to qualify new commodity servers for Rubrik-branded Appliances, this may create increased costs or delays for our customers and impact their customer experience, which could negatively impact our sales and our business. See the section titled "Business—Manufacturing" in our Annual Report for additional information regarding our contractual relationship with Supermicro.

Certain of our OEMs carry products that compete with our solutions and may not continue producing or supporting compatible commodity servers for our customers in the future. We or our Channel Partners provide forecasts and purchase orders to Manufacturers for compatible commodity servers, and these orders may only be rescheduled or canceled under certain limited conditions. If we inaccurately forecast demand for our solutions and need for compatible commodity servers, our Manufacturers may have excess or inadequate inventory, and we may incur cancellation charges or penalties, which could adversely impact our operating results. If we experience increased demand for compatible commodity servers, then we, our Channel Partners, or Manufacturers may need to increase component purchases, contract manufacturing capacity, or internal test and quality functions. Our customers' orders may represent a relatively small percentage of the overall orders received by Manufacturers from their customers. As a result, fulfilling our customers' orders may not be considered a priority in the event Manufacturers are constrained in their ability to fulfill all of their customer obligations in a timely manner. Although we have largely transitioned the sale of Rubrik-branded Appliances from us to our contract manufacturers, if Manufacturers are unable to provide adequate supplies of high-quality products, or if we, our Channel Partners, or Manufacturers are unable to obtain adequate quantities of components, or control the costs of components, it could cause a delay in the fulfillment of our customers' orders, in which case our business, financial condition, and results of operations could be adversely affected.

Tariffs and other restrictive trade policies, such as those regarding hardware and technology infrastructure from China, have had and may continue to have an indirect impact on the total price customers pay for our products and may also impact production and supply of our Rubrik-branded Appliances and the commodity servers compatible with our solutions. These impacts could negatively affect customer experience, demand, and the attractiveness of our solutions relative to alternatives.

Our use of generative, agentic and other AI tools may pose risks to business and operations, including our proprietary software and systems, and may subject us to legal liability.

We use and increasingly rely upon AI tools in our business, including generative AI and agentic AI, including to generate code and other materials incorporated into our products, proprietary software, and systems, and for other internal and external uses, and we are making investments to expand our generative and agentic AI capabilities, including recent and future product offerings such as Rubrik Agent Cloud, which is designed to accelerate enterprise AI agent deployments. Advanced generative AI tools, which may produce content indistinguishable from that generated by humans, are a relatively novel development, with benefits, risks, and liabilities still unknown. Recent decisions of governmental entities and courts (such as the U.S. Copyright Office, U.S. Patent and Trademark Office, and U.S. Court of Appeals for the Federal Circuit) interpret U.S. copyright and patent law as limited to protecting works and inventions created by human authors and inventors, respectively. We are therefore unlikely to be able to obtain U.S. copyright or patent protection for works or inventions wholly created by a generative AI tool, and our ability to obtain U.S. copyright and patent protection for source code, text, images, inventions, or other materials, which are developed with some use of generative AI tools, may be limited, if available at all. Likewise, the availability of such IP protections in other countries is unclear. In addition, we may have little or no insight into and no control over the content and materials used by vendors and model providers to train these generative AI tools, or that otherwise use or incorporate these generative AI tools into their own offerings. There is ongoing litigation over whether the use of copyrighted materials to train the AI models used in these tools is lawful, and the impact of decisions in such litigation on our use of generative AI tools is unknown. Furthermore, our vendors who use generative and agentic AI tools in their own offerings may not meet existing or rapidly evolving regulatory or industry standards, including with respect to the rights of others, privacy and data security. Additionally, our use of open-source and other third-party generative and agentic AI tools, including to develop source code, text, images, inventions, or other materials, may expose us to greater risks than utilizing contracted human developers, as such AI tools typically do not come with warranties or indemnities with respect to the output generated by such AI tools, and generative and agentic AI tools may also hallucinate, providing erroneous output or making erroneous decisions. Furthermore, some AI tools may be offered under terms that do not protect the confidentiality of the prompts or inputs that users submit to such tools and may use prompts or inputs to train shared AI models, potentially resulting in third-party users receiving outputs containing information from prompts or inputs (including confidential, competitive, proprietary, or personal data) that we submitted to the tool. The disclosure and use of personal data in AI technologies is also subject to various privacy laws and other privacy obligations. Prior to implementing an AI tool (including generative AI tools), our AI governance committee (including leaders from our Engineering, Product, Legal, and Information Security teams) performs an analysis and review of each AI tool for which pre-approval is required according to our policies, including evaluation of potential legal, security, and business risks and steps that can be taken to mitigate any such risks. The selection criteria and analysis include consideration of how use of the AI tool could raise issues relating to confidential information, personal data and privacy, customer data and contractual obligations, open source software, copyright and other intellectual property rights, transparency, output accuracy and reliability, and security.

Additionally, while we employ practices designed to evaluate, track, and mitigate risk around our use of third-party AI tools, our practices may not be error free, and our use of such tools may inadvertently violate a third party's rights, be non-compliant with the applicable terms of use or our other legal obligations, or result in a security or privacy risk or data leakage. Our use of AI technology could result in additional compliance costs, regulatory investigations and actions, and lawsuits. For example, we may face new or enhanced governmental scrutiny, or claims from third parties claiming infringement of their intellectual property rights or mandatory compliance with open-source software or other license terms with respect to software or other materials or content we believed to be available for use and not subject to license terms or other third-party proprietary rights. Any of these claims could result in legal investigations or proceedings. Furthermore, if we are found to be in violation of third party rights based on our use of AI tools, we could be required to purchase costly licenses, comply with the requirements of third-party licenses, or limit or cease using the implicated software or other materials or content, unless and until we can re-engineer such software, materials, or content to avoid infringement or change the use of, or remove, the implicated third-party materials, which could reduce or eliminate the value of our technologies and services. Our use of generative and agentic AI tools to generate code may also present additional risks in a variety of contexts, such as the risk generated source code may contain security vulnerabilities, bugs, or other unexpected behavior. The use of agentic AI tools also poses a security risk to our information technology environment, as effective integration of agentic AI tools into our product development and other internal workflows may involve provisioning agentic AI tools with access to and the ability to modify certain of our systems and data, meaning that a compromise, misuse, unauthorized access to, or other unintended use of such an agentic AI tool could have adverse impacts on large portions of our systems and data. Furthermore, the rapid evolution of AI technologies may at times outpace the development of effective security controls that account for the risks such technologies introduce. Though we take efforts designed to mitigate risks introduced by AI technologies, our efforts may not always be successful, particularly for novel or emerging risks. Moreover, certain of the AI tools we currently, or may in the future, use are developed and maintained by third parties, and such technologies may not be designed, tested, or validated for deployment in enterprise environments as complex as ours. Though we perform due diligence into third-party providers of AI tools and, where appropriate, impose contractual requirements regarding their information security practices, we may not be able to control the way third-party products or services are developed, trained or

maintained. Due to the rapid evolution of AI tools (including generative AI and agentic AI), such tools may perform unexpectedly in our enterprise environment, and could result in downtime or otherwise introduce cybersecurity vulnerabilities. Additionally, vendors of AI tools may fail to comply with their contractual obligations to us regarding the confidentiality or security of any data or other inputs provided to such vendor or outputs generated by their AI tools. Our sensitive information or that of our customers could be leaked, disclosed, or revealed as a result of or in connection with our employees', personnel's, or vendors' use of third-party AI technologies.

We also market some of our own products or features as generative AI tools and AI infrastructure services ("AI Products"). Some of our customers, especially those in highly regulated industries, may be reluctant or unwilling to adopt AI Products. Accordingly, adoption of AI features in our products and marketing our products as AI Products could reduce or delay customer adoption. Because AI models and AI agents can hallucinate and provide erroneous output or make erroneous decisions, offering AI Products could result in customer dissatisfaction or potentially claims against us arising out of erroneous output or decisions. Some of our AI Products may require us to train or fine-tune AI models using datasets collected by us or from third-party providers. While we have processes and practices designed to ensure that we and any third-party providers of training data have the necessary rights to use such datasets for training our AI Products, we may not in every instance be able to confirm that all of the information contained in such datasets has been obtained with the necessary permissions for us to use for purposes of our AI Products. For example, we may use publicly available data to train our AI Products that contain information that was unlawfully acquired from third parties without our knowledge. While we have employed processes designed to help us avoid using any personal data to train or fine-tune our AI Products, it may be difficult for us to avoid or identify all instances where a user might nonetheless submit personal data to our AI Products. Furthermore, if we were to receive claims from third parties asserting rights against our use of certain datasets used to train our AI Products, it may be difficult or impossible for us to disentangle our trained models from the subject matter of the claims.

Our AI Products may also rely on certain third party providers of AI technology. Our success in deploying AI features and tools for our AI Products is reliant on these third parties and their platforms. We cannot control the quality, availability or pricing of such third-party platforms, especially in a highly competitive environment. If any such third-party platforms become incompatible with our offerings or unavailable for use or have degradations in performance, or if the providers of such models unfavorably change the terms on which their AI platforms are offered or terminate their relationship with us, our solutions may become less appealing to our customers. In addition, for any third party providers of AI platforms that host platforms on our behalf any disruption, outage, or loss of information, data breaches, cybersecurity threats or other data loss through such hosted services could disrupt our operations or solutions, damage our reputation, cause a loss of confidence in our solutions, or result in legal claims or proceedings, for which we may be unable to recover damages from the affected provider.

Several jurisdictions around the globe, including in Europe, have proposed, enacted, or are considering laws governing AI tools, including the EU's AI Act. In the United States, where our operations are headquartered, several states are applying their data and consumer protection laws to AI, and/or have enacted, or are enacting or considering legal frameworks on AI, such as the California Bot Disclosure Law, the Utah Artificial Intelligence Policy Act, the Colorado Artificial Intelligence Act and the CCPA's regulations regarding automated decision-making technology. We expect other jurisdictions will adopt similar laws, and, as a result of the rapidly evolving regulatory landscape, implementation standards, enforcement practices, and available scope of protection are likely to remain uncertain for the foreseeable future, and we cannot yet determine the impact future laws, regulations, or standards may have on our business (including our positioning with respect to our competition) and may not always be able to anticipate how to respond to these laws or regulations. Additionally, certain privacy laws extend rights to consumers (such as the right to delete certain personal data) and regulate automated decision making, which may be incompatible with our use of AI. These obligations may make it harder for us to conduct our business using AI, lead to regulatory fines or penalties, require us to disclose or provide greater transparency regarding the nature of our AI Products and the data we have employed to train them, require us to change our business practices, retrain our AI Products, or prevent or limit our use of AI. For example, the FTC has required other companies to delete (or "disgorge") both the personal data that the FTC alleged were collected in violation of privacy laws as well as the algorithms and other insights that were developed or generated using such data. If we cannot use AI or that use is restricted, our business may be less efficient, or we may be at a competitive disadvantage.

Also, the rapid evolution of AI technologies may require the expenditure of significant resources to design, develop, test and maintain our products and services to help ensure that our AI features and tools are implemented in accordance with applicable law and regulation and in a socially responsible manner and to minimize any real or perceived unintended harmful impacts. We also may need to expend further resources to adjust our business practices, as these laws and regulations evolve, especially where requirements across jurisdictions are inconsistent.

Any of these risks could be difficult to eliminate or manage, and, if not addressed, could adversely affect our business, financial condition, results of operations, and growth prospects.

Changes in our revenue mix may cause fluctuations in revenue recognized from period to period, which could make period-to-period revenue comparisons not meaningful and difficult to predict.

Our revenue mix may vary over time due to a number of factors, including the mix of our subscriptions for different data security products and the timing of remaining customer migrations to RSC or other SaaS offerings. Our subscription revenue includes revenue from sales of subscription term-based licenses, a portion of which is recognized upfront when we transfer control of the subscription term-based license to the customer, and revenue from sales of SaaS subscriptions and support, which is recognized ratably over the contract period. As we have substantially completed our transition from subscription term-based licenses to SaaS subscriptions and migrated a significant majority of our existing customers to RSC, the proportion of revenue recognized upfront versus ratably over time has evolved. However, the timing of remaining customer migrations, as well as the estimates and assumptions used to account for certain customer arrangements, including Subscription Credits (which are customer options that are accounted for as material rights) related to Refresh Rights, may continue to affect the amount and timing of revenue recognized. In addition, future changes in our product offerings, pricing models, contract structures, customer purchasing patterns, or other business initiatives may further affect our revenue mix and the timing of revenue recognized. These factors make it challenging to forecast our revenue as the mix of solutions and services, the timing of our customers' RSC transition, as well as the size of contracts, are difficult to predict.

We rely upon third-party cloud providers to host our solutions, and any disruption of, or interference with, our use of third-party cloud products would adversely affect our business, financial condition, and results of operations.

Customers of RSC and our other cloud services need to be able to access our solutions at any time, without interruption or degradation of performance, and we provide them with service-level commitments with respect to uptime. We leverage third-party cloud providers for substantially all of the infrastructure that supports our solutions. Our cloud services depend on the cloud infrastructure hosted by these third-party providers to support our configuration, architecture, features, and interconnection specifications, as well as secure the information stored in these virtual data centers, which is transmitted through third-party internet service providers. Any limitation on the capacity of our third-party hosting providers, including due to technical failures, shifts in product capabilities or licensing models, natural disasters, fraud, global conflicts or security attacks, could impede our ability to fulfill our current contractual commitments, onboard new customers, or expand the usage of our existing customers, which could adversely affect our business, financial condition, and results of operations.

In addition, third-party cloud providers run their own platforms that we access, and we are, therefore, vulnerable to their service interruptions. We have in the past and may in the future experience interruptions, delays, and outages in service and availability from time to time as a result of problems with our third-party cloud providers' infrastructure. Lack of availability of this infrastructure could be due to a number of potential causes that we cannot predict or prevent, including technical failures, natural disasters, fraud, or cyber security attacks. Such outages could lead to the triggering of our service-level commitments and extensions of affected services at no charge to our customers, which may impact our business, financial condition, and results of operations. In addition, if our security, or that of any of these third-party cloud providers, is compromised, our software is unavailable, or our customers are unable to use our software within a reasonable amount of time or at all, our business, financial condition, and results of operations could be adversely affected. In some instances, we may not be able to identify the cause or causes of these performance problems within a period of time acceptable to our customers. It is possible that our customers and potential customers would hold us accountable for any breach of security affecting a third-party cloud provider's infrastructure, and we may incur significant liability from those customers and from third parties with respect to any breach affecting these systems. We may not be able to recover a material portion of our liabilities to our customers and third parties from a third-party cloud provider. It may also become increasingly difficult to maintain and improve our performance, especially during peak usage times, as our software becomes more complex and the usage of our software increases. Any of the above circumstances or events may harm our business, financial condition, and results of operations.

We may not be able to successfully manage our growth, and if we are not able to grow efficiently, our business, financial condition, and results of operations could be harmed.

As usage and adoption of our platform and data security products grow, we will need to devote additional resources to improving our capabilities, features, and functionality. In addition, we will need to appropriately scale our internal business operations and our services organization to serve our growing customer base. Any failure of or delay in these efforts could result in impaired product performance and reduced customer satisfaction, resulting in decreased sales to new customers, lower average subscription dollar-based net retention rates, or the issuance of service credits or requested refunds, which would hurt our revenue growth and our reputation. Further, any failure in optimizing the costs associated with use of third-party cloud services as we scale could negatively impact our margins. Our expansion efforts will be expensive and complex and will require the dedication of significant management time and attention. We could also face inefficiencies, vulnerabilities, or service disruptions as a result of our efforts to scale our internal infrastructure, which may result in extended outages, loss of customer trust, and harm to our reputation. We cannot be sure that the

expansion of and improvements to our internal infrastructure will be effectively implemented on a timely basis, if at all, and such failures could harm our business, financial condition, and results of operations.

The markets in which we participate are competitive, and if we do not compete effectively, our business, financial condition, and results of operations could be harmed.

The data security market is new and intensely competitive, characterized by rapidly changing technology and evolving standards, changing customer requirements, and frequent new product introductions. Our main competitors fall into the following categories:

- Data management and protection vendors, such as Dell-EMC, IBM, Commvault, Veeam, and Cohesity;
- Cloud and SaaS data management vendors with products that compete in some of our markets; and
- Vendors that provide cyber/ransomware detection and investigation, data security posture management, identity security posture management, Active Directory and Entra ID security and protection, insider threat detection, data classification, and other data security or data governance technologies.

The principal competitive factors in our industry include product functionality, product integration, platform coverage, ability to scale, price, worldwide sales infrastructure, global technical support, labor and development costs, name recognition, and reputation. The ability to converge data security and data management in a cloud architecture is also a significant competitive factor in our industry. If we are unable to address these factors, our competitive position could weaken, and we could experience a decline in revenue that could adversely affect our business.

Many of our current and potential competitors have longer operating histories and may have substantially greater financial, technical, sales, marketing, and other resources than we do, as well as larger installed customer bases, greater name recognition, lower labor and development costs, and broader product solutions, including servers. Some of these competitors can devote greater resources to the development, promotion, sale, and support of their data security products than we can. As a result, these competitors may be able to respond more quickly to new or emerging technologies and changes in customer requirements. For example, many of our competitors are also investing in AI technology to improve their data security products, which could enable them to respond more quickly to new or emerging threats and changes in customer requirements.

It is also costly and time-consuming to change data management systems. Most of our new or potential customers have already installed data management systems, which gives an incumbent competitor an advantage in retaining a customer due to significant risk to data continuity from switching vendors. The incumbent competitor already understands the data, applications, network infrastructure, user demands, and information technology needs of the customer, such that some customers are reluctant to invest the time, money, and resources necessary to implement configuration, integration, training, and other operational complexities that arise from another vendor. In addition, for any of our existing customers that have not yet transitioned to RSC, any perceived negative impacts or incremental costs associated with the transition to RSC, or a more rapid transition than planned by the customer, may result in customer dissatisfaction and give our competitors an opportunity to acquire these customers.

Our current and potential competitors may establish cooperative relationships among themselves or with third parties or may merge with each other. If so, new competitors, alliances, or merged entities that include our competitors may emerge that could acquire significant market share. In addition, large operating systems, applications, and cloud vendors have introduced products or functionality that include some of the same functions offered by our solutions. In the future, further development by these vendors could cause our solutions to become redundant, which could seriously harm our business, financial condition, and results of operations.

In addition, we expect to encounter new competitors, including public cloud providers and SaaS companies that build native data security and management solutions, as we expand in current markets or enter new markets. Furthermore, many of our existing competitors are broadening their operating systems platform coverage. We expect that competition will increase as a result of future software industry consolidation. Increased competition could harm our business by causing, among other things, price reductions of our solutions, reduced profitability, and loss of market share.

Our estimates of market opportunity, forecasts of market growth, and potential return on investment may prove to be inaccurate, and even if the market in which we compete achieves the forecasted growth, our business could fail to grow at similar rates, if at all.

Market opportunity estimates and growth forecasts, whether obtained from third-party sources or developed internally, are subject to significant uncertainty and are based on assumptions and estimates that may not prove to be accurate. The markets in which we operate are at an early stage and are rapidly evolving. These markets include data management, data security, identity, and AI. As a result, the size and future growth of this market are difficult to accurately estimate and subject to change. In addition, third-party estimates of the addressable market for the markets in which we operate reflect the opportunity available from all participants and

potential participants, and we cannot predict with precision our ability to address this demand or the extent of market adoption of our solutions. Moreover, the market segments we are targeting may grow at different rates. The variables that go into the calculation of our market opportunity are subject to change over time, and there is no guarantee that any particular number or percentage of addressable businesses covered by our market opportunity estimates will purchase our solutions or generate any particular level of revenue for us. Any expansion in our market opportunity depends on a number of factors, including the cost, performance, and perceived value associated with our solutions and the products of our competitors. Even if the areas in which we compete achieve the forecasted growth, our business could fail to grow at similar rates, if at all.

If customers have not utilized their Subscription Credits before they expire, this could result in customer dissatisfaction and our future results of operations could be harmed.

The customer enterprise data we secure relies upon compatible hardware. Historically, we sold Rubrik-branded Appliances produced by contract manufacturers to our customers. We started transitioning the sale of Rubrik-branded Appliances from us to our contract manufacturers in fiscal 2023 and offered limited-time incentives, Subscription Credits (which are customer options that are accounted for as material rights), upon qualification, to certain existing customers in exchange for historically offered rights to next generation Rubrik-branded Appliances at no cost, which we refer to as Refresh Rights. If customers have not utilized their Subscription Credits before they expire, this could result in customer dissatisfaction or a decision not to purchase our solutions, which would have an adverse impact on our results of operations.

We rely on the performance of highly skilled personnel, including senior management and engineering, services, sales, and technology professionals. If we are unable to retain or motivate key personnel or hire, retain, and motivate qualified personnel, our business will be harmed.

We believe our success has depended, and continues to depend, on the efforts and talents of our senior management team, particularly Bipul Sinha, our Chairman of our board of directors, Chief Executive Officer, and co-founder, and Arvind Nithrakashyap, our Chief Technology Officer and co-founder, as well as our other key employees in the areas of research and development and sales and marketing.

From time to time, there may be changes in our senior management team or other key employees resulting from the hiring or departure of these personnel. Our executive officers and certain other key employees are employed on an at-will basis, which means that these personnel could terminate their employment with us at any time. The loss of one or more of our executive officers, or the failure by our executive team to effectively work with our employees and lead our company, could harm our business. We also are dependent on the continued service of our existing software engineers because of the complexity of our solutions. In addition, a significant portion of our software engineers are located in Palo Alto, California and Bangalore, India. These locations offer access to a deep pool of highly skilled professionals, which is crucial for the development and maintenance of our complex solutions. However, this concentration also exposes us to potential continuity risk if these specific locations are negatively impacted by unforeseen events, such as natural disasters, political unrest, or disruptions in critical infrastructure.

In addition, to execute our growth plan, we must attract and retain highly qualified personnel. Competition for these personnel is intense, especially for engineers experienced in designing and developing cloud-based infrastructure products, for experienced sales professionals, and for cybersecurity professionals. If we are unable to attract such personnel at appropriate locations, we may need to hire in new regions, which may add to the complexity and costs of our business operations. From time to time, we have experienced, and we expect to continue to experience, difficulty in hiring and retaining employees with appropriate qualifications. Many of the companies with which we compete for experienced personnel have greater resources than we have. As has occurred in the past, if we hire employees from competitors or other companies, their former employers may attempt to assert that these employees or we have breached certain legal obligations, resulting in a diversion of our time and resources. In addition, prospective and existing employees often consider the value of the equity awards they receive in connection with their employment. If the perceived value of our equity awards declines, experiences significant volatility, or increases such that prospective employees believe there is limited upside to the value of our equity awards, it may adversely affect our ability to recruit and retain employees. If we fail to attract new personnel or fail to retain and motivate our current personnel, our business and growth prospects would be harmed.

We derive substantially all of our revenue from our data security platform. Failure of our platform to satisfy customer demands or achieve continued market acceptance over competitors would harm our business, financial condition, results of operations, and growth prospects.

We derive substantially all of our revenue from our platform, and we have directed, and intend to continue to direct, a significant portion of our financial and operating resources to developing more features and functionality for our platform.

Our growth will depend in large part on our ability to attract new customers and expand sales to existing customers, expand the features and functionality of our platform, hire sufficient sales personnel to support our growth, and decrease the ramp time for our sales personnel. In addition, the success of our business is substantially dependent on the actual and perceived viability, benefits, and advantages of our platform. As such, market adoption of our platform, data security and agentic AI operations solutions is critical to our continued success. Demand for our platform and data security products is affected by a number of factors, including increased market acceptance by new and existing customers, increased market acceptance of our AI offerings, such as Rubrik Agent Cloud, increased activity by or prevalence of cybersecurity bad actors, including the use of ransomware, effectiveness of our sales and marketing strategy, the extension of our platform to new applications and use cases, the timing of development and release of new capabilities by us and our competitors, technological change, and growth or contraction of the market in which we compete. Failure to successfully address or account for these factors, satisfy customer demands, achieve continued market acceptance over competitors, and achieve growth in sales of our data security products would harm our business, financial condition, results of operations, and growth prospects.

We expect fluctuations in our financial results, making it difficult to project future results, and if we fail to meet the expectations of securities analysts or investors with respect to our results of operations, our stock price and the value of your investment could decline.

Our results of operations have fluctuated in the past and are expected to fluctuate in the future due to a variety of factors, many of which are outside of our control. As a result, our past results may not be indicative of our future performance. In addition to the other risks described herein, factors that may affect our results of operations include:

- changes in our revenue mix;
- changes in actual and anticipated growth rates of our revenue, customers, and key operating metrics;
- fluctuations in demand for or pricing of our solutions;
- our ability to attract new customers;
- the level of awareness and prevalence of cybersecurity threats, particularly advanced cyberattacks and ransomware attacks;
- timing of our customers exercising or forfeiting their Subscription Credits (which are customer options that are accounted for as material rights), including the impact on our revenue recognition and causing fluctuations to our total revenue growth and limit the comparability of our revenue with past performance;
- our ability to retain our existing customers, particularly large customers, and secure renewals of subscriptions, as well as the timing of customer renewals or non-renewals;
- the pricing and quantity of subscriptions renewed, as well as our ability to accurately forecast customer expansions and renewals;
- downgrades in customer subscriptions;
- customers and potential customers opting for alternative solutions, including developing their own in-house solutions;
- timing and amount of our investments to expand the capacity of our third-party cloud service providers;
- seasonality in sales, results of operations, and remaining performance obligations;
- investments in new offerings, including protection of new enterprise, cloud, SaaS, unstructured data, identity providers, new features, and functionality;
- fluctuations or delays in development, release, or adoption of new features and functionality for our solutions;
- delays in closing sales, including the timing of renewals, which may result in revenue being pushed into the next fiscal quarter, particularly because a large portion of our sales occur toward the end of each fiscal quarter;
- fluctuations or delays in purchasing decisions in anticipation of new data security products or enhancements by us or our competitors;
- changes in customers' budgets, the timing of their budget cycles and purchasing decisions, and payment schedules;
- our customers' ability to procure Rubrik-branded Appliances or compatible commodity servers from Manufacturers, particularly in light of supply chain constraints that have resulted in extended lead times and increased server prices, and any commercial accommodations we may provide in response;
- the number of qualified customers that elect to utilize their Subscription Credits (which are customer options that are accounted for as material rights) before they expire;
- our ability to control costs, including hosting costs and our operating expenses;
- the amount and timing of payment for operating expenses, particularly research and development and sales and marketing expenses, including commissions;
- timing of hiring personnel for our research and development and sales and marketing organizations;
- the amount and timing of non-cash expenses, including stock-based compensation expense and other non-cash charges;

- the amount and timing of costs associated with recruiting, educating, and integrating new employees and retaining and motivating existing employees;
- the effects of acquisitions and their integration;
- general economic conditions, both domestically and internationally, as well as economic conditions specifically affecting industries in which our customers participate;
- fluctuations in foreign currency exchange rates;
- the impact of new accounting pronouncements;
- changes in regulatory or legal environments that may cause us to incur, among other things, expenses associated with compliance;
- the impact of changes in tax laws or judicial or regulatory interpretations of tax laws, which are recorded in the period such laws are enacted or interpretations are issued and may significantly affect the effective tax rate of that period and following periods;
- health epidemics or pandemics;
- changes in the competitive dynamics of our market, including consolidation among competitors or customers; and
- significant security incidents related to, technical difficulties with, or interruptions to, the delivery and use of our solutions.

Any of these and other factors, or the cumulative effect of some of these factors, may cause our results of operations to vary significantly. If our quarterly results of operations fall below the expectations of investors and securities analysts who follow our stock, the price of our Class A common stock could decline substantially, and we could face costly lawsuits, including securities class action suits.

In addition, while we recognize our SaaS subscription revenue ratably over the term of the subscription, our customers typically pay us for new multi-year subscriptions upfront and then annually upon one-year renewals. Recently, due to the growth in our SaaS product offerings, changes in our customer mix, and the uncertain macroeconomic environment, we have experienced an increase in customers electing annual, monthly, or consumption payments instead of multi-year upfront payments, which has caused and may continue to cause volatility in our period over period cash flow and may have an adverse effect on our business and results of operations.

Our ability to introduce new data security products and features is dependent on adequate research and development resources and our ability to successfully complete acquisitions. If we do not adequately fund our research and development efforts or complete acquisitions successfully, we may not be able to compete effectively, and our business and results of operations may be harmed.

To remain competitive, we must continue to offer new data security products and enhancements to our platform and existing solutions. This is particularly true as we further expand and diversify our capabilities. Maintaining adequate research and development resources, such as the appropriate personnel and development technology, to meet the demands of the market is essential. If we elect not to or are unable to develop solutions internally due to certain constraints, such as high employee turnover, lack of management ability, or a lack of other research and development resources, we may choose to expand into a certain market or strategy via an acquisition for which we could potentially pay too much or fail to successfully integrate into our operations. Further, many of our competitors expend a considerably greater amount of funds on their respective research and development programs, and those that do not may be acquired by larger companies that would allocate greater resources to our competitors' research and development programs. Our failure to maintain adequate research and development resources or to compete effectively with the research and development programs of our competitors would give an advantage to such competitors, and our business, financial condition, and results of operations could be adversely affected. Moreover, there is no assurance that our research and development or acquisition efforts will successfully anticipate market needs and result in significant new marketable solutions or enhancements to our solutions, design improvements, cost savings, revenues, or other expected benefits. If we are unable to generate an adequate return on such investments, we may not be able to compete effectively, and our business and results of operations may be adversely affected.

We depend and rely on SaaS technologies and cloud infrastructure services from third parties to operate our business, and interruptions or performance problems with these technologies may adversely affect our business and results of operations.

We rely on hosted SaaS applications and cloud infrastructure services from third parties in order to operate critical functions of our business, including AI-built applications, enterprise resource planning, order management, billing, project management, human resources, technical support, accounting, and other operational activities. If these services become unavailable due to extended outages, interruptions, or because they are no longer available on commercially reasonable terms, our expenses could increase, our ability to manage finances could be interrupted, and our processes for managing sales of our solutions and supporting our customers could be impaired until equivalent services, if available, are identified, obtained, and implemented, all of which could adversely affect our business and results of operations.

If we are unable to maintain successful relationships with our Channel Partners and technology alliance partners, or if our Channel Partners or technology alliance partners fail to perform, our ability to market, sell, and distribute our solutions will be limited, and our business, financial condition, and results of operations will be harmed.

In addition to our sales force, we rely on our Channel Partners, which include our managed service providers and distributors and resellers, to sell and support our solutions. A vast majority of sales of our solutions flow through our Channel Partners with the support of our sales force. Our three largest Channel Partners, Arrow Enterprise Computing Solutions, Exclusive Networks, and Ingram Micro Inc., and their respective affiliates collectively generated approximately 68% and 73% of our revenue for fiscal 2026 and 2025, respectively. Our agreements with our Channel Partners, including our agreements with our three largest Channel Partners, are non-exclusive, renew automatically in one-year term increments, and may be terminated by either party at any time. Further, our Channel Partners fulfill our sales on a purchase order basis and do not impose minimum purchase requirements or related terms on sales. Our Channel Partners enable us to extend our reach, in particular with smaller customers and in geographies where we have less sales presence. Additionally, we have entered, and intend to continue to enter, into technology alliance partnerships with third parties to support our future growth plans.

We derive a substantial amount of our revenue from sales through Channel Partners, and we expect to continue to derive a substantial amount of our revenue from Channel Partners in future periods. Our agreements with our Channel Partners are generally non-exclusive and do not prohibit them from working with our competitors or offering competing products, and many of our Channel Partners may have more established relationships with our competitors. If our Channel Partners choose to place greater emphasis on solutions other than our own, fail to effectively market and sell our solutions, or fail to meet the needs of our customers, then our ability to grow our business and sell our solutions may be adversely affected. In addition, the loss of one or more of our larger Channel Partners or technology alliance partners, who may cease marketing our solutions with limited or no notice, and any inability to replace them, could adversely affect our business, financial condition, and results of operations. Moreover, our ability to expand our distribution channels depends in part on our ability to maintain successful relationships with our Channel Partners and educate and train our current and future Channel Partners about our solutions, which can be complex. If we fail to effectively manage our existing sales channels, or if our Channel Partners are unsuccessful in fulfilling the orders for our solutions, or if we are unable to enter into arrangements with, and retain a sufficient number of, high quality Channel Partners in each of the regions in which we sell solutions and keep them motivated to sell our solutions, our business, financial condition, and results of operations will be harmed. Even if we are successful, these relationships may not result in greater customer usage of our data security products or increased revenue. Our ability to influence, or have visibility into, the actions or efforts of our Channel Partners may be limited. If our partners, including our Channel Partners, fail to comply with applicable laws, including anti-corruption, export control and sanctions, antitrust, or competition laws, or engage in activities that result in or may result in liability, we may also be adversely affected through reputational harm, as well as other negative consequences, including litigation, government investigations and penalties.

In addition, the financial health of our Channel Partners and our continuing relationships with them are important to our success. Some of these Channel Partners may be unable to withstand adverse changes in economic conditions, including the current macroeconomic uncertainty, which could result in insolvency or the inability of such Channel Partners to obtain credit to finance purchases of our solutions and services. In addition, weakness in the end-user market could negatively affect the cash flows of our Channel Partners who could, in turn, delay paying their obligations to us, which would increase our credit risk exposure. Our business could be harmed if the financial condition of some of these Channel Partners substantially weakened, and we were unable to timely secure replacement Channel Partners.

If we do not effectively expand and train our sales force, we may be unable to add new customers or retain and increase sales to our existing customers, and our business will be adversely affected.

We depend on our sales force to obtain new customers and retain and increase sales with existing customers. Our ability to achieve significant revenue growth will depend, in large part, on our success in recruiting, training, and retaining sufficient numbers of sales personnel, as well as effectively managing leadership transitions and maintaining stability within our sales organization. Changes in sales leadership or organizational structure may result in temporary disruption, changes in strategy or execution, or challenges in maintaining sales team morale and productivity, and may increase the risk of attrition within our sales organization, including the potential loss of key sales personnel. We have expanded our sales organization significantly in recent periods and expect to continue to add additional sales capabilities in the near term. There is significant competition for sales personnel with the skills and technical knowledge that we require. New hires require significant training and may take significant time before they achieve full productivity, and this delay is accentuated by our long sales cycles. Our recent hires and planned hires may not become productive as quickly as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do or plan to do business. In addition, a large percentage of our sales force is new to our company and selling our solutions, and therefore, this group may be less effective than our more seasoned sales personnel. Furthermore, hiring sales personnel in new countries, or expanding our existing presence, requires upfront and ongoing expenditures that we may not recover if the sales personnel fail to achieve full

productivity. We cannot predict whether, or to what extent, our sales will increase as we expand our sales force or how long it will take for sales personnel to become productive. If we are unable to hire and train a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or retaining and increasing sales to our existing customer base, our business, financial condition, and results of operations will be adversely affected.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense.

Our revenue may fluctuate because of the length and unpredictability of the sales cycle for our solutions, particularly with respect to large organizations and government entities. For example, in light of current macroeconomic conditions, such as higher cost-consciousness around information technology budgets, as well as constraints affecting the availability or pricing of compatible commodity servers needed to deploy our solutions, including as a result of global chip shortages or allocation constraints, we have observed a lengthening of our sales cycles. Customers often view the subscription to our platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test, and qualify our platform, including from a security and privacy perspective, prior to entering into or expanding a relationship with us. Large enterprises and government entities in particular often undertake a significant evaluation process that further lengthens our sales cycle. Additionally, RSC and other SaaS solutions may elongate our sales cycles as a result of additional customer security and privacy evaluations.

Our sales team develops relationships with our customers and works with our Channel Partners on account penetration, account coordination, sales, and overall market development. We spend substantial time and resources on our sales efforts without any assurance that our efforts will produce a sale. Data security product purchases are frequently subject to budget constraints, multiple approvals, and unanticipated administrative, processing, and other delays. As a result, it is difficult to predict whether and when a sale will be completed.

If we fail to adapt and respond effectively to rapidly changing technology, including technologies related to AI, evolving industry standards, changing regulations, or to changing customer needs, requirements, or preferences, our solutions may become less competitive.

Our ability to attract new users and customers and increase revenue from existing customers depends in large part on our ability to enhance, improve, and differentiate our existing offering, increase adoption and usage of our solutions, and introduce new products and capabilities. The market in which we compete is relatively new and subject to rapid technological change, including advances in AI, evolving industry standards, and changing regulations, as well as changing customer needs, requirements, and preferences. The success of our business will depend, in part, on our ability to adapt and respond effectively to these changes on a timely basis. Because the market for our data security solutions is relatively new, it is difficult to predict customer adoption, increased customer usage and demand for our data security solutions, the size and growth rate of this market, the entry of competitive products, or the success of existing competitive products. If we are unable to enhance our solutions and keep pace with rapid technological change, including developments related to AI and automated systems, or if new technologies emerge that are able to deliver competitive products at lower prices, more efficiently, more conveniently, or more securely than our solutions, our business, financial condition, and results of operations could be adversely affected.

To remain competitive, we need to continuously modify and enhance our solutions to adapt to changes and innovation in existing and new technologies. We expect that we will need to continue to differentiate our data management and data security capabilities, as well as expand and enhance our data security and AI solutions to support a variety of use cases. This development effort will require significant engineering, sales, and marketing resources. Any failure to effectively offer solutions for these adjacent use cases could reduce customer demand for our platform. Further, our solutions must also integrate with a variety of network, commodity appliance, mobile, cloud, and software platforms and technologies, and we need to continuously modify and enhance our solutions to adapt to changes and innovation in these technologies. This development effort may require significant investment in engineering, support, marketing, and sales resources, all of which would affect our business and results of operations. Any failure of our solutions to operate effectively with widely adopted data infrastructure platforms, applications, and technologies would reduce the demand for our solutions. If we are unable to respond to customer demand in a cost-effective manner, our solutions may become less marketable and less competitive or obsolete, and our business, financial condition, and results of operations could be adversely affected.

The competitive position of our solutions depends in part on their ability to operate with third-party products and services, including those of our technology alliance partners, and if we are not successful in maintaining and expanding the compatibility of our solutions with such products and services, our business may be harmed.

The competitive position of our solutions depends in part on their ability to operate with products and services of third parties, including software companies, software services, and infrastructure, and our solutions must be continuously modified and enhanced to adapt to changes in commodity appliance, software, networking, browser, and database technologies. In the future, one or more technology companies, whether our technology alliance partners or otherwise, may choose not to support the operation of their software, software

services, and infrastructure with our solutions, or our solutions may not support the capabilities needed to integrate with such software, software services, and infrastructure. In addition, to the extent that a third party was to develop software or services that compete with ours, that provider may choose not to support our offering. We intend to facilitate the compatibility of our platform with various third-party software, software services, and infrastructure offerings by maintaining and expanding our business and technical relationships. If we are not successful in achieving this goal, our business, financial condition, and results of operations may be harmed.

Incorrect or improper implementation or use of our solutions could result in customer dissatisfaction and harm our business, financial condition, and results of operations.

Our solutions are deployed in a wide variety of IT infrastructures, including large-scale, complex technology environments, and we believe our future success will depend, at least in part, on our ability to support such deployments. Implementations of our solutions may be technically complicated, and it may not be easy to maximize the value of our solutions without proper implementation, training, and support. Some of our customers have experienced difficulties implementing our solutions in the past and may experience implementation difficulties in the future. If we or our customers are unable to implement our solutions successfully, customer perceptions of our solutions may be impaired, our reputation and brand may suffer, or customers may choose not to renew their subscriptions or purchase additional products from us.

Any failure by customers to appropriately implement our solutions or any failure of our solutions to effectively integrate and operate within our customers' data management infrastructure could result in customer dissatisfaction, impact the perceived reliability of our solutions, result in negative press coverage, negatively affect our reputation, and harm our business, financial condition, and results of operations.

We use third-party open-source components in our solutions, which could negatively affect our ability to sell our solutions or subject us to litigation or other actions.

Our solutions include third-party open-source components, including software and models, and we intend to continue to incorporate third-party open-source components in our solutions in the future. There is a risk that the use of third-party open-source components in our software could impose conditions or restrictions on our ability to monetize our software or require making available the source code of all or part of our software that include, incorporate or rely upon such open-source components. Although we have internal policies in place designed to monitor the incorporation of open-source components into our solutions to avoid such restrictions, we cannot be certain that we have not incorporated open-source components in our solutions in a manner that is inconsistent with our licensing model or the licensing terms of any such open-source components. Open-source software is incorporated into or relied upon by many other software projects, including open source projects as well as AI tools, and there is a risk that those dependent open-source libraries may be subject to inconsistent licensing terms that affect our ability to use the software. This could create further uncertainties as to the governing terms for the open-source components we incorporate.

In addition, the terms of certain open-source licenses to which we are subject have not been interpreted by U.S. or foreign courts, and there is a risk that open-source licenses could be construed in a manner that imposes unanticipated restrictions or conditions on our use of such components. Additionally, we may from time to time face claims from third parties claiming ownership of, or demanding release of, the software or derivative works that we developed using such open-source components, which could include proprietary portions of our source code, or otherwise seeking to enforce the terms of the open-source licenses. These claims could result in litigation and could require us to make those proprietary portions of our source code freely available, purchase a costly license or cease offering the implicated software or services unless and until we can re-engineer them to avoid infringement. This re-engineering process could require significant additional research and development resources, and we may not be able to complete it successfully.

In addition to risks related to license requirements, use of third-party open-source components can lead to greater risks than use of third-party commercial components, as open-source licensors generally do not provide warranties. Use of open-source components may also introduce security risks as it may contain security vulnerabilities, and hackers and other third parties may exploit the public availability of such open-source components to determine how to compromise our solutions.

In addition, licensors of open-source components included in our solutions may, from time to time, modify the terms of their license agreements applicable to any updates in such a manner that those license terms may include restrictions that make the use of such components incompatible with our business, and thus could, among other consequences, prevent us from using or incorporating new updates of such components that are subject to the modified license.

In addition, any source code that we contribute to open-source projects becomes publicly available, subject to the relevant open source license. As a result, our ability to protect some of our intellectual property rights in such source code may be limited or lost entirely, and we would be unable to prevent our competitors or others from using such contributed source code in accordance with the relevant open source license.

Any of these risks could be difficult to eliminate or manage, and if not addressed, could have a negative effect on our business, financial condition, and results of operations.

Our success depends, in part, on the integrity and scalability of our systems and infrastructures. System interruption or delays from third-party data center hosting facilities and the lack of integration, redundancy, and scalability in our systems and infrastructures could impair the delivery of our solutions and harm our business.

Our success depends, in part, on our ability to maintain the integrity of our systems and infrastructure, including websites, information, and related systems. System interruption and the lack of integration and sufficient redundancy in our information systems and infrastructures may harm our ability to operate websites, respond to customer inquiries, and generally maintain cost-efficient operations. We may experience occasional system interruptions that make some or all systems or data unavailable or prevent us from efficiently providing solutions.

We currently utilize third-party data center hosting facilities located in the United States and internationally. Any damage to, or failure of, the data facilities generally could result in interruptions in our solutions. As we continue to add data center hosting facilities and add capacity in our existing data facilities, we may move or transfer our data and our customers' data. Despite precautions taken during this process, any unsuccessful data transfers may impair the delivery of our solutions. We also rely on affiliate and third-party computer systems, broadband, and other communications systems and service providers in connection with the provision of services generally, as well as to facilitate, process, and fulfill transactions. Interruptions in our solutions may reduce our revenue, cause us to issue credits or pay penalties, cause customers to terminate their subscriptions or solutions contracts, or harm our renewal rates or our ability to attract new customers. Our business will also be harmed if our customers and potential customers believe our solutions are unreliable.

Fire, flood, power loss, telecommunications failure, hurricanes, tornadoes, earthquakes, acts of war or terrorism, acts of God, and similar events or disruptions may damage or interrupt computer, broadband, or other communications systems and infrastructures at any time. Any of these events could cause system interruption, delays, and loss of critical data, and could prevent us from providing our solutions. While we have backup systems for certain aspects of our operations, disaster recovery planning by its nature cannot be sufficient for all eventualities. In addition, we may not have adequate insurance coverage to compensate for losses from a major interruption. As we continue to expand the number of our customers and solutions products available to our customers, we may not be able to scale our technology to accommodate the increased capacity requirements, which may result in interruptions or delays in the delivery or performance of our solutions. If any of these events were to occur, it could harm our business, financial condition, and results of operations.

We rely on software and data licensed from other parties. Defects in or the loss of software or access to data from third parties could increase our costs and harm the quality of our solutions.

Components of our solutions include or rely upon software and data licensed from third parties. Our business could be disrupted if any of the software or data we license from others and functional equivalents thereof were either no longer available to us or no longer offered on commercially reasonable terms. In either case, we may be required to either redesign our solutions to function with software or data available from other parties or develop these components ourselves, which would result in increased costs and could result in delays in the release of new solutions. Furthermore, we might be forced to limit the features available in our current or future data security or AI solutions. If we fail to maintain or renegotiate any of these software or data licenses, we could face significant delays and diversion of resources in attempting to license and integrate functional equivalents. While we believe that in most cases there are commercially reasonable alternatives to the third-party software and data we currently license, this may not always be the case, or it may be time consuming or expensive to replace existing third-party software or data or find a replacement third-party provider. Our use of additional or alternative third-party software or data or third-party providers would require us to enter into license agreements with third parties, and we may not be able to enter into such agreements on advantageous terms.

We are subject to governmental export and import controls and economic sanctions laws and regulations that could impair our ability to compete in international markets or subject us to liability and reputational harm if we violate the controls.

Our data security solutions are subject to U.S. export controls, including the Export Administration Regulations, and we incorporate encryption technology into our solutions. Our data security solutions and the underlying technology may be exported outside of the United States only in compliance with the applicable regulations and any required export authorizations, including an export license, applicability of a license exception, or other appropriate government authorizations, such as the filing of an encryption classification request or self-classification report, as applicable. Obtaining the necessary export license or other authorization for a particular sale may be time-consuming and may result in the delay or loss of sales opportunities.

Furthermore, we are required to comply with economic and trade sanctions laws and regulations of the countries where we do business, including those administered and enforced by the U.S. government (for example, through the Office of Foreign Assets Control)

of the U.S. Treasury Department and the U.S. Department of State). These economic and trade sanctions prohibit or restrict the provisions of products and services to embargoed jurisdictions and sanctioned persons, unless otherwise authorized.

While we have taken certain precautions to prevent our solutions and related technology and services from being provided in violation of trade controls and are in the process of enhancing our compliance policies and procedures relating to trade controls, our solutions may have been in the past, and could in the future be, provided inadvertently and/or without our knowledge in violation of such trade control laws and regulations. Violations of U.S. trade controls or other applicable laws/regulations can result in significant fines or penalties and possible criminal liability for responsible employees and managers, in addition to potential reputational harm.

If our partners, including our Channel Partners, fail to obtain appropriate import, export, or re-export licenses or permits, we may also be adversely affected through reputational harm, as well as other negative consequences, including government investigations and penalties.

Also, various countries, in addition to the United States, regulate the import and export of certain encryption software and related technology, including import and export licensing requirements, and have enacted laws that could limit our ability to distribute our solutions or could limit our customers' ability to implement our solutions in those countries. Changes in our solutions or future changes in export and import regulations may create delays in the introduction of our solutions in international markets, prevent our customers with international operations from deploying our solutions globally or, in some cases, prevent the export or import of our solutions to certain countries, governments, or persons altogether. From time to time, various governmental agencies have proposed, and are expected to implement additional regulation of encryption technology.

Any change in export or import regulations, economic sanctions, or related laws or regulations, or change in the countries, governments, persons, or technologies targeted by such regulations, could result in decreased use of our solutions by, or in our decreased ability to export or sell our solutions to, existing or potential customers. Any decreased use of our solutions or limitation on our ability to export or sell our solutions would adversely affect our business, financial condition, results of operations, and growth prospects.

We are subject to anti-corruption, anti-bribery, and similar laws, and non-compliance with such laws can subject us to criminal or civil liability and harm our business, financial condition, and results of operations.

We are subject to the U.S. Foreign Corrupt Practices Act ("FCPA"), U.S. domestic bribery laws, the UK Bribery Act, and other anti-corruption and anti-bribery laws in the countries in which we conduct business. Anti-corruption and anti-bribery laws are interpreted broadly to prohibit companies, their officers and employees, and their third-party intermediaries from authorizing, offering, or providing, or in some cases receiving, directly or indirectly, improper payments or benefits to or from persons in the public or private sector. As a public company, we are also required by the FCPA to keep accurate books and records and maintain internal accounting controls sufficient to assure management's control, authority, and responsibility over our assets. As we engage in and increase our international business and sales to the public sector, we may engage with business partners and third-party intermediaries, including Channel Partners, to market and sell our solutions and to obtain necessary permits, licenses, and other regulatory approvals from government authorities. In addition, we or our third-party intermediaries may have direct or indirect interactions with officials, employees, or other representatives of government agencies or state-owned or affiliated entities. We can be held liable for the corrupt or other illegal activities of these third-party intermediaries and our employees, representatives, contractors, partners, and agents, even if we do not explicitly authorize or have actual knowledge of such unlawful activities.

While we have policies and procedures and conduct training designed to address compliance with such laws, our employees and agents may take actions in violation of our policies and applicable law, for which we may be ultimately held responsible. As we increase our international sales and business, our risks under these laws may increase.

Detecting, investigating, responding to, and resolving actual or alleged violations of anti-corruption laws can lead to a materially significant diversion of time, resources, and attention from senior management, as well as significant defense costs and other professional fees. In addition, noncompliance with anti-corruption and anti-bribery laws, could subject us to whistleblower complaints, investigations, sanctions, settlements, prosecution, enforcement actions, fines, damages, other civil or criminal penalties or injunctions, suspension, or debarment from contracting with certain persons, reputational harm, adverse media coverage, and other collateral consequences. If any subpoenas or investigations are launched, or governmental or other sanctions are imposed, or if we do not prevail in any possible civil or criminal proceeding, our business, financial condition, and results of operations could be harmed.

Downturns or upturns in our sales may not be immediately reflected in our financial condition and results of operations.

We recognize a significant portion of our revenue ratably over the term of subscriptions to our solutions. As a result, any decreases in new subscriptions or renewals in any one period may not immediately be fully reflected as a decrease in revenue for that period but would negatively affect our revenue in future quarters. This also makes it difficult for us to rapidly increase our revenue through the sale

of additional subscriptions in any period. If our quarterly results of operations fall below the expectations of investors and securities analysts who follow our stock, the price of our Class A common stock would decline substantially, and we could face costly lawsuits, including securities class actions.

Seasonality may cause fluctuations in our revenue and related metrics.

Historically, we have experienced seasonality in revenue and related metrics, as we typically sell a higher percentage of subscriptions to new customers, and expansion and renewal subscriptions with existing customers in the fourth quarter of our fiscal year. We believe that this results from the procurement, budgeting, and deployment cycles of many of our customers, particularly our enterprise customers. We expect that this seasonality may continue to affect our revenue and related metrics in the future and might become more pronounced as we continue to target enterprise customers.

Our subscription annual recurring revenue (“Subscription ARR”), cloud annual recurring revenue (“Cloud ARR”), and certain other operational data are operating metrics that are subject to assumptions and limitations, including that the factors that impact Subscription ARR will vary from those that impact subscription revenue. As such, these metrics may not provide an accurate indication of our actual performance or our future results.

Subscription ARR, Cloud ARR, and other non-GAAP operational metrics are based on numerous assumptions and limitations, are calculated using our internal data from non-financial systems, have not been independently audited by third party financial audit firms as is typical for GAAP financials, and may not accurately reflect actual financial results nor provide an accurate indication of future or expected results. Further, the definitions and assumptions for these metrics may differ from those calculated by other businesses. Subscription ARR and Cloud ARR are not proxies for revenue or forecasts of revenue, and do not reflect any anticipated reductions in contract value due to contract non-renewals or service cancellations. In addition, the factors that impact Subscription ARR will vary from those that impact subscription revenue in a given period. As a result, Subscription ARR, Cloud ARR, and our other operational data may not accurately reflect our actual financial performance, and investors should consider these metrics in light of the assumptions and processes used in calculating such metrics and the limitations as a result thereof. Investors should not place undue reliance on these metrics as an indicator of our future or expected results. Moreover, these metrics may differ from similarly titled metrics presented by other companies and may not be comparable to such other metrics. See the section titled “Management’s Discussion and Analysis of Financial Condition and Results of Operations—Key Business Metrics” for additional information regarding Subscription ARR, Cloud ARR, and other operational metrics.

We will face risks associated with the growth of our business with certain heavily regulated industry verticals.

We market and sell our solutions to customers in heavily regulated industry verticals, including the banking, healthcare, and financial services industries. As a result, we face additional regulatory scrutiny, risks, and burdens from the governmental entities and agencies that regulate those industries. Entering new heavily regulated verticals and expanding in those verticals in which we are already operating will continue to require significant resources to address potential regulatory scrutiny, risks, and burdens, and there is no guarantee that such efforts will be successful or beneficial to us. If we are unable to successfully penetrate these verticals, maintain our market share in such verticals in which we already operate, or cost-effectively comply with governmental and regulatory requirements applicable to our activities with customers in such verticals, our business, financial condition, and results of operations may be harmed.

Sales to government entities are subject to a number of challenges and risks.

We sell to U.S. federal, state, and local, as well as foreign governmental agency customers. Sales to such entities are subject to a number of challenges and risks. Selling to such entities can be highly competitive, expensive, and time-consuming, often requiring significant upfront time and expense without any assurance that these efforts will generate a sale. Government contracting requirements may change and in doing so restrict our ability to sell into the government sector until we have obtained any required government certifications. Further, achieving and maintaining government certifications, such as U.S. Federal Risk and Authorization Management Program (“FedRAMP”) certification for our data security solutions, may require significant upfront and ongoing cost, time, and resources. If we do not maintain our existing FedRAMP certification or obtain additional certifications for our data security solutions, we may not be able to sell certain solutions to the U.S. federal government and public sector customers as well as eligible private sector customers that require such certification for their intended use cases, which could harm our growth, business, and results of operations. This may also harm our competitive position against larger enterprises whose competitive data security solutions are certified. Further, there can be no assurance that we will secure commitments or contracts with government entities even following such certifications, which could harm our margins, business, financial condition, and results of operations. Government demand and payment for our data security solutions are affected by public sector budgetary cycles, procurement policies and funding authorizations, with funding reductions or delays, including in connection with an extended government shutdown, adversely affecting public sector demand for our data security solutions.

Further, governmental entities may demand contract terms that differ from our standard arrangements and are less favorable than terms agreed with private sector customers. Such entities may have statutory, contractual, or other legal rights to terminate contracts with us or our Channel Partners for convenience or for other reasons. Any such termination may adversely affect our ability to contract with other government customers as well as our reputation, business, financial condition, and results of operations. Governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our subscriptions, a reduction of revenue, or fines or civil or criminal liability if the audit uncovers improper or illegal activities, which could adversely affect our business, financial condition, results of operations, and reputation.

In January 2025, the current administration began issuing executive orders identifying new government policy and directing U.S. federal agencies to evaluate their current actions, including certain spending, to ensure that such actions are consistent with the new administration's priorities. Some of those executive orders as well as other agency designations, such as supply-chain risk designations, are the subjects of pending litigation, and there remains significant uncertainty about the ways in which agencies will implement the new executive orders and agency designations. Such implementation could negatively affect our current and future business with U.S. government agencies.

Our customers also include certain non-U.S. governments, to which government procurement law risks similar, and in some cases potentially contradictory, to those present in U.S. government contracting also apply, particularly in certain emerging markets where our customer base is less established. In addition, compliance with complex regulations and contracting provisions in a variety of jurisdictions can be expensive and consume significant management resources. In certain jurisdictions, our ability to win business may be constrained by political and other factors unrelated to our competitive position in the market. These difficulties could harm our business, financial condition, and results of operations. In addition, we must also comply with other government regulations related to employment practices, environmental protection, health and safety, tax, accounting, and anti-fraud measures, as well as many other regulations in order to maintain our government contractor status. For example, as a government contractor, we maintain plans to ensure compliance with nondiscrimination and regulatory requirements for qualified employees on the basis of gender, race, disability, and veteran status. Consequently, we may be subject to executive orders and regulatory changes affecting various aspects of our operations, including compliance with nondiscrimination plans. Any required elimination or modification of such plans in response to new executive orders could pose challenges in hiring or retaining employees, and may lead to other adverse operational impacts.

In October 2023, we received a grand jury subpoena from the Department of Justice, U.S. Attorney's Office for the District of Maryland ("DOJ"), which requested information regarding two specific companies, which we subsequently learned were associated with an employee from one of our sales teams who is no longer with the company and who was indicted by a federal grand jury in the District of Maryland in October 2024 and is being prosecuted by the DOJ. We are fully cooperating with this investigation and have been conducting our own thorough internal investigation. In the course of our internal investigation, we have discovered communications among certain employees within one of our sales teams, including such former Rubrik employee, that relate to potential violations of federal law in connection with government contracts, and are similarly cooperating with the DOJ with respect to these matters. These investigations are ongoing, and we do not know when they will be completed, the entirety of facts we will ultimately discover as a result of the investigations, or what actions the government may or may not take. We cannot predict the ultimate outcome of these investigations and the full extent of potential consequences. A negative outcome in any or all of these matters could cause us to incur substantial fines, penalties, or other financial exposure, as well as reputational harm and exclusion from future contracting with the federal government.

Acquisitions, strategic investments, joint ventures, or alliances could be difficult to identify, pose integration challenges, divert the attention of management, disrupt our business and culture, dilute stockholder value, and adversely affect our business, financial condition, and results of operations.

We have in the past and may in the future seek to acquire or invest in businesses, joint ventures, products and platform capabilities, technologies, or technical know-how that we believe could complement or expand our platform capabilities, enhance our technical capabilities, or otherwise offer growth opportunities. Any such acquisition or investment may divert the attention of management and cause us to incur various expenses in identifying, investigating, and pursuing suitable opportunities, whether or not the transactions are completed, and may result in unforeseen operating difficulties and expenditures. In particular, we may encounter difficulties assimilating or integrating the businesses, technologies, products and platform capabilities, personnel, or operations of any acquired companies, particularly if the key personnel of an acquired company choose not to work for us, their software is not easily adapted to work with our solutions, or we have difficulty retaining the customers of any acquired business due to changes in ownership, management, or otherwise. These transactions may also disrupt our business, divert our resources, and require significant management attention that would otherwise be available for development of our existing business. We may also have difficulty establishing our company values with personnel of acquired companies, which may negatively impact our culture and work environment. Any such transactions that we are able to complete may not result in any synergies or other benefits we had expected to achieve, which could result in impairment

charges that could be substantial. In addition, we may not be able to find and identify desirable acquisition targets or business opportunities or be successful in entering into an agreement with any particular strategic partner. These transactions could also result in dilutive issuances of equity securities or the incurrence of debt, which could adversely affect our results of operations. In addition, if the resulting business from such a transaction fails to meet our expectations, our business, financial condition, and results of operations may be adversely affected, or we may be exposed to unknown risks or liabilities.

Any inability to maintain a high-quality customer support organization could lead to a lack of customer satisfaction, which could hurt our customer relationships and have an adverse effect on our business, financial condition, and results of operations.

Once our solutions are deployed, customers rely on our technical support services to assist with service customization and optimization and to resolve certain issues relating to the implementation and maintenance of our solutions. Customers also rely on our or our Channel Partners' support personnel to resolve issues and realize the full benefits that our solutions provide. If we or our Channel Partners do not effectively assist customers in deploying our solutions, succeed in helping customers quickly resolve technical issues or provide effective ongoing support, our ability to sell additional solutions as part of our platform to existing customers would be adversely affected, and our reputation with potential customers could be damaged.

In addition, our sales process is highly dependent on our product and business reputation and on positive recommendations from existing customers. Any failure to maintain high-quality technical support, or a market perception that we do not maintain high-quality technical support, could adversely affect our reputation, our ability to sell our services to existing and prospective customers, and our business, financial condition, and results of operations.

Our business is subject to the risks of warranty and product liability claims from real or perceived defects in our solutions or their misuse by customers or third parties and indemnity provisions in various agreements that potentially expose us to substantial liability for intellectual property infringement and other losses.

We may in the future be subject to liability claims for damages related to undetected defects, errors, or vulnerabilities in our solutions. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our platform could harm our business, financial condition, and results of operations. Although we generally have limitation of liability provisions in our terms and conditions, in rare cases we have agreed to limited exceptions to such liability caps, and such limitation of liability provisions may not fully or effectively protect us from claims as a result of federal, state, or local laws or ordinances, or unfavorable judicial decisions in the United States or other countries.

Moreover, as part of our ransomware recovery warranty (the "Ransomware Recovery Warranty"), we also provide certain customers with up to \$10,000,000 for recovery expenses related to data recovery and restoration in the event that data backed up using our solutions cannot be recovered following a ransomware attack. As part of the Ransomware Recovery Warranty, if an eligible customer's data that has been backed up onto a Rubrik-branded Appliance, Rubrik-certified compatible third-party commodity server, or a Rubrik-hosted cloud platform, is not successfully recovered by way of one of our data security products due to a failure of such solution, we will reimburse the customer for its reasonable and necessary fees and expenses to restore, recover, or recreate its data up to \$10,000,000. If many of our customers experience security incidents or other incidents that fall within this program and we are not able to recover their data through our data security solutions, we could be required to pay significant amounts to comply with our obligations under the Ransomware Recovery Warranty. In the event that we are required to regularly provide financial assistance for such recovery activities, and particularly if we have to do so for multiple customers at the same or similar times, this could significantly increase our costs, harm our reputation and brand, and increase the costs to us associated with this warranty program, which could adversely affect our business, financial condition, and results of operations.

Additionally, we typically provide indemnification to customers for certain losses suffered or expenses incurred as a result of third-party claims arising from our infringement of a third party's intellectual property. We also may be exposed to liability for certain breaches of confidentiality or customer data, as defined in our terms of service which, as a standard practice, are generally subject to caps on liability. We also assume limited liability in the event we breach certain of our terms of service. Certain of these contractual provisions survive termination or expiration of the applicable agreement. We have not received any material indemnification claims from third parties. However, as we continue to grow, the possibility of these claims against us will increase.

If customers or other third parties with whom we do business make intellectual property infringement or other indemnification claims against us, we will incur significant legal expenses and may have to pay damages, license fees, or stop using technology found to be in violation of a third party's rights. We may also have to seek a license for the technology. Such licenses may not be available on reasonable terms, if at all, and may significantly increase our operating expenses or may require us to restrict our business activities and limit our ability to deliver certain solutions or features. We may also be required to develop alternative non-infringing technology, which could either require significant effort and expense or cause us to alter our solutions, or both, which could harm our business.

Large indemnity obligations, whether for intellectual property or in certain limited circumstances, other claims, would harm our business, financial condition, and results of operations.

Under certain circumstances, our personnel may have access to customer platforms. An employee may take advantage of such access to conduct malicious activities or fail to follow internal policies or make errors that could cause system failures, loss of data, or other adverse effects on our customers. Misuse of our solutions by our personnel could result in claims from our customers for damages related to such misuse. Such misuse of our solutions could also result in negative press coverage and negatively affect our reputation, which could result in harm to our reputation, business, financial condition, and results of operations. In addition, misuse of our solutions could also result in contractual breaches and damages to customers that may assert warranty and other claims for substantial damages against us.

We maintain insurance to protect against certain claims associated with the use of our solutions, but our insurance coverage may not adequately cover any claim asserted against us and is subject to deductibles. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert management's time and other resources, and harm our reputation, business, financial condition, and results of operations.

Failure to effectively develop and expand our sales and marketing capabilities or improve the productivity of our sales and marketing organization could harm our ability to expand our potential customer and sales pipeline, increase our customer base, and achieve broader market acceptance of our solutions.

Our ability to increase our customer base, achieve broader market adoption and acceptance of our solutions, and expand our potential customer and sales pipeline and brand awareness will depend to a significant extent on our ability to expand and improve the productivity of our sales and marketing organization. We plan to continue expanding our sales force, both domestically and internationally. We also plan to dedicate significant resources to sales and marketing programs to decrease the time required for our sales personnel to achieve desired productivity levels, which may be impacted in the short term from our new approach to sales force segmentation. Historically, newly hired sales personnel have needed several quarters to achieve desired productivity levels. Our increased sales and marketing efforts will also involve investing significant financial and other resources, which could result in increased costs and negatively impact margins. We are one of the only providers of a unified data security platform, so we must therefore invest heavily in our sales and marketing functions in order to educate customers and potential customers about our solutions. Our business and results of operations will be harmed if our sales and marketing efforts fail to successfully expand our potential customer and sales pipeline, including through increasing brand awareness, new customer acquisition, and market adoption of our platform and solutions, particularly for RSC, or fail to generate significant increases in revenue or result in increases that are smaller than anticipated. We may not achieve anticipated revenue growth from expanding our sales force if we are unable to hire, develop, integrate, and retain talented and effective sales personnel, if our new and existing sales personnel, on the whole, are unable to achieve desired productivity levels in a reasonable period of time or at all, or if our sales and marketing programs are not effective.

If we fail to enhance our brand cost-effectively, our ability to expand our customer base will be impaired and our business, financial condition, and results of operations may be adversely affected.

We believe that developing and maintaining awareness of our brand in a cost-effective manner is critical to achieving widespread acceptance of our existing and future solutions for data security and agentic AI operations and is an important element in attracting new customers. In addition, creating brand awareness of our data security and agentic AI operations solutions will require added investment in our marketing and branding activities. We believe that the importance of brand recognition will increase as competition in our market increases. Successful promotion of our brand will depend largely on the effectiveness of our marketing efforts and on our ability to develop and deploy high-quality, reliable, and differentiated data security and agentic AI operations solutions to our customers. In the past, our efforts to build our brand have involved significant expense. Brand promotion activities may not yield increased revenue, and even if they do, any increased revenue may not offset the expense we incur in building our brand. If we fail to successfully promote and maintain our brand or incur substantial expense in an unsuccessful attempt to promote and maintain our brand, we may fail to attract new customers or retain our existing customers to the extent necessary to realize a sufficient return on our brand-building efforts, and our business, financial condition, and results of operations could be adversely affected.

We have a limited history with pricing models for our solutions, and we may need to adjust the pricing terms of our data security solutions, which could have an adverse effect on our revenue and results of operations.

We have limited experience with respect to determining the optimal prices for our offerings across an expanding portfolio of solutions and capabilities, including new offerings and subscriptions to and renewals of our solutions and new subscription editions. As the markets in which we operate evolve, or as new competitors introduce new products or services that compete with ours, we may be unable to attract new customers. In the past, we have been able to increase our prices for our solutions, but we may choose not to introduce or be unsuccessful in implementing future price increases. Furthermore, since we have limited experience pricing our product

suites, RSC and RAC, as well as new products we may introduce from time to time, we may be unsuccessful in implementing future price increases and our future pricing power may erode due to changing market dynamics, increased competition, ability to sell to information security teams, or other factors. As a result of these and other factors, in the future we may be required to reduce our prices or be unable to increase our prices, or it may be necessary for us to increase our services or solutions without additional revenue to remain competitive, all of which could harm our financial condition and results of operations.

We may require additional capital to support the growth of our business, and this capital might not be available on acceptable terms, if at all.

We have funded our operations since inception primarily through equity and debt financings and sales of our solutions. We cannot be certain when or if our operations will generate sufficient cash to fully fund our ongoing operations or the growth of our business. We intend to continue to make investments to support our business, which may require us to engage in further equity or debt financings to secure additional funds. Additional financing may not be available on terms favorable to us, if at all, particularly during times of market volatility, higher interest rates, inflationary pressures, and general economic instability. If adequate funds are not available on acceptable terms, we may be unable to invest in future growth opportunities, which could harm our business, financial condition, and results of operations. Any debt we incur could give the debt holders rights senior to our stockholders to make claims on our assets and could involve covenants which may limit our ability to obtain additional capital, pursue business opportunities and strategic transactions and pay dividends on our Class A common stock. For example, the holders of our Notes have rights senior to holders of our Class A common stock to make claims on our assets, and the indenture governing the Notes, include customary covenants for us, such as covenants to make payment of principal and special interest (if any) and remain current in our reporting obligations with the SEC. Furthermore, if we issue additional equity securities, including shares of Class A common stock issued upon conversion of the Notes, stockholders will experience dilution, and in some cases we may issue new equity securities that have rights senior to those of our Class A common stock. Because our decision to issue securities in the future will depend on numerous considerations, including factors beyond our control, we cannot predict or estimate the amount, timing, or nature of any future issuances of debt or equity securities. As a result, our stockholders bear the risk of future issuances of debt or equity securities reducing the value of our Class A common stock and diluting their interests.

Servicing our debt may require a significant amount of cash. We may not have sufficient cash flow from our business to pay our indebtedness.

Our ability to make scheduled payments of the principal of, to pay special interest, if any, on or to refinance the Notes, depends on our future performance, which is subject to economic, financial, competitive and other factors beyond our control. Our business may not continue to generate sufficient cash flow from operations to service our debt and make necessary capital expenditures. If we are unable to generate such cash flow, we may be required to adopt one or more alternatives, such as selling assets, restructuring debt, or obtaining additional equity capital on terms that may be onerous or highly dilutive. Our ability to refinance the Notes will depend on the capital markets and our financial condition at such time. We may not be able to engage in any of these activities or engage in these activities on desirable terms, which could result in a default on our debt obligations. In addition, any of our future debt agreements may contain restrictive covenants that may prohibit us from adopting any of these alternatives. Our failure to comply with these covenants could result in an event of default which, if not cured or waived, could result in the acceleration of our debt repayment.

We may not have enough available cash or the ability to raise the funds necessary to pay cash upon conversion of the Notes or to repurchase the Notes upon a fundamental change.

Holders of the Notes will have the right, subject to certain conditions and limited exceptions, to require us to repurchase all or any portion of their Notes upon the occurrence of a fundamental change (as defined and described in the Indenture). In addition, upon any conversion of the Notes, unless we elect to deliver solely shares of our Class A common stock to settle such conversion, we will be required to make cash payments in respect of the Notes being converted. However, we may not have enough available cash or be able to obtain financing at the time we are required to make repurchases of Notes surrendered therefor or pay cash with respect to Notes being converted. Our failure to repurchase the Notes at a time when the repurchase is required by the Indenture or to pay any cash payable on future conversions of the Notes as required by the Indenture would constitute a default under the Indenture. If the repayment of the related indebtedness were to be accelerated, we may not have sufficient funds to repay the indebtedness and repurchase the Notes or make cash payments upon conversions of the Notes.

We are exposed to fluctuations in currency exchange rates, which could negatively affect our results of operations.

Our solutions are billed in U.S. dollars, and therefore, our revenue is not subject to foreign currency risk. However, a strengthening of the U.S. dollar could increase the real cost of our solutions to our customers outside of the United States and negatively impact sales to foreign customers. Alternatively, if the U.S. dollar weakens, our operating expenses could rise, which could adversely affect our results of operations. In addition, an increasing portion of our operating expenses are incurred outside the United States. These operating

expenses are denominated in foreign currencies and are subject to fluctuations due to changes in foreign currency exchange rates. While we do not currently hedge against the risks associated with currency fluctuations, if our foreign currency risk increases in the future and we are not able to successfully hedge against the risks associated with currency fluctuations, our results of operations could be adversely affected.

Unfavorable conditions in our industry or the global economy, including those caused by the ongoing conflicts around the world, or reductions in technology spending, could limit our ability to grow our business and negatively affect our results of operations.

Global business activities face widespread macroeconomic uncertainties, and our results of operations may vary based on the impact of changes in our industry or the global economy on us or our customers and potential customers. Negative conditions in the general economy both in the United States and abroad, including conditions resulting from changes in gross domestic product growth, financial and credit market fluctuations, inflation and efforts to control further inflation, including high interest rates, bank failures, international trade relations, including tariffs and trade tensions, political turmoil, military conflicts, U.S. federal government shutdowns, natural catastrophes, warfare, and terrorist attacks could cause a decrease in business investments by existing or potential customers, including spending on technology, and negatively affect the growth of our business. In addition to the foregoing, adverse developments that affect financial institutions, transactional counterparties, or other third parties, such as bank failures or concerns or speculation about any similar events or risks, could lead to market-wide liquidity problems, which in turn may cause third parties, including our customers, to become unable to meet their obligations under various types of financial arrangements as well as general disruptions or instability in the financial markets. Such economic volatility could adversely affect our business, financial condition, results of operations, and cash flows, and future market disruptions could negatively impact us. In particular, we have experienced and may continue to experience longer sales cycles and related negotiations for prospective customers and existing customer expansions, a reduction in multi-year upfront payments for our subscription offerings, reduced contract sizes or generally increased scrutiny on technology spending and budgets from existing and potential customers, due in part to the effects of macroeconomic uncertainty. These customer dynamics may persist in the future, even if macroeconomic conditions improve, and to the extent there is a sustained general economic downturn, a recession, or another situation where technology budgets grow at a slower rate or contract, these customer dynamics may be exacerbated. In addition to the foregoing, we have operations in Israel, which have been affected and may continue to be affected by the ongoing conflict in Israel and the Middle East, and our growth, business, and results of operations could be further negatively impacted if the current conflict in Israel and the Middle East continues, worsens, or expands to other nations or regions. Similarly, we have a significant presence in Bangalore, India, which may be disrupted by future conflicts between India and Pakistan, potentially leading to development delays and operational interruptions to our software engineering and renewals teams. Our competitors, many of whom are larger and have greater financial resources than we do, may respond to challenging market conditions by lowering prices in an attempt to attract our customers, which may require us to respond in kind and may negatively impact our existing customer relationships and new customer acquisition strategy. In addition, the increased pace of consolidation in certain industries may result in reduced overall spending on our solutions. We cannot predict the timing, strength, or duration of any economic slowdown, instability, or recovery, generally or within any particular industry.

We typically provide service-level commitments under our customer agreements. If we fail to meet these commitments, we could face customer terminations, a reduction in renewals, and damage to our reputation, which would lower our revenue and harm our business, financial condition, and results of operations.

Our agreements with our customers typically provide for service-level commitments relating to service availability. If we fail to meet these commitments, we could be required to extend affected services at no charge and could face customer terminations, or a reduction in renewals, which could significantly affect both our current and future revenue. Any service-level commitment failures could also damage our reputation. The complexity and quality of our customers' implementation and the performance and availability of cloud services and cloud infrastructure are outside our control, and therefore, we are not in full control of whether we can meet these service-level commitments. Our business, financial condition, and results of operations could be adversely affected if we fail to meet our service-level commitments for any reason. Any extended service outages could adversely affect our business, reputation, and brand.

Sales to enterprise customers involve risks that may not be present or that are present to a lesser extent with respect to sales to smaller organizations.

We are seeing an increasing volume of sales to large, enterprise customers. Sales to enterprise customers and large organizations involve risks that may not be present or that are present to a lesser extent with sales to smaller customers, including the commercial customer segment. These risks include longer sales cycles and negotiations, more complex customer requirements (including audit and other requirements driven by such customers' regulatory and industry contexts), substantial upfront sales costs, and less predictability in completing some of our sales. For example, enterprise customers may require considerable time to evaluate and test our solutions and those of our competitors prior to making a purchase decision and placing an order or may need specialized security features to

meet regulatory requirements. A number of factors influence the length and variability of our sales cycle, including the need to educate potential customers about the uses and benefits of our solutions, the discretionary nature of purchasing and budget cycles, the macroeconomic uncertainty and challenges and resulting increased technology spending scrutiny, and the competitive nature of evaluation and purchasing approval processes. Since the processes for deployment, configuration, and management of our solutions are complex, we are also often required to invest significant time and other resources to train and familiarize potential customers with our solutions. Customers may engage in extensive evaluation, testing, and quality assurance work before making a purchase commitment, which increases our upfront investment in sales, marketing, and deployment efforts, with no guarantee that these customers will make a purchase or increase the scope of their subscriptions. In certain circumstances, an enterprise customer's decision to use our solutions may be an organization-wide decision, and therefore, these types of sales require us to provide greater levels of education regarding the use and benefits of our solutions. As a result, the length of our sales cycle, from identification of the opportunity to deal closure, has varied, and may continue to vary, significantly from customer to customer, with sales to large enterprises and organizations typically taking longer to complete. Moreover, large enterprise customers often begin to deploy our solutions on a limited basis but nevertheless demand configuration, integration services, and pricing negotiations, which increase our upfront investment in the sales effort with no guarantee that these customers will deploy our solutions widely enough across their organization to justify our substantial upfront investment.

Given these factors, it is difficult to predict whether and when a sale will be completed and when revenue from a sale will be recognized due to the variety of ways in which customers may purchase our solutions. This may result in lower than expected revenue in any given period, which would have an adverse effect on our business, financial condition, and results of operations.

Our intellectual property rights may not adequately protect our business.

To be successful, we must protect our technology, know-how, and brand in the United States and other jurisdictions through trademarks, trade secrets, patents, copyrights, service marks, invention assignments, contractual restrictions, and other intellectual property rights and confidentiality procedures. Despite our efforts to implement these protections, they may not adequately protect our business for a variety of reasons, including:

- our inability to successfully register or obtain patents, trademarks, and other intellectual property rights that sufficiently protect our brand and the full scope of important innovations;
- any inability by us to maintain appropriate confidentiality and other protective measures to establish and maintain our trade secrets;
- uncertainty in, and evolution of, legal standards relating to the validity, enforceability, and scope of protection of intellectual property rights;
- potential invalidation of our intellectual property rights through administrative processes or litigation;
- other practical, resource, or business limitations on our ability to detect and prevent infringement or misappropriation of our rights and to enforce our rights; and
- uncertainty with respect to legal standards regarding the existence, validity and enforceability of proprietary rights in outputs from AI platforms (including those that we may use for coding our products and tools).

Further, the laws of certain foreign countries, particularly certain developing countries, do not provide the same level of protection of corporate proprietary information and assets, such as intellectual property, including trademarks, trade secrets, know-how, and records, as the laws of the United States and mechanisms for enforcement of intellectual property rights may be inadequate. As a result, we may encounter significant problems in protecting and defending our intellectual property or proprietary rights abroad. Additionally, we may also be exposed to material risks of theft or unauthorized reverse engineering of our proprietary information and other intellectual property, including software source code, designs, specifications, or other sensitive information. Our efforts to enforce our intellectual property rights in such foreign countries may be inadequate to obtain a significant commercial advantage from the intellectual property that we develop, which could have an adverse effect on our business, financial condition, and results of operations. Moreover, if we are unable to prevent the disclosure of our trade secrets to third parties, or if our competitors independently develop any of our trade secrets, we may not be able to establish or maintain a competitive advantage in our market, which could seriously harm our business.

We also contribute to open-source projects. Although we have internal policies and procedures designed to pre-approve the incorporation of any of our source code into open-source projects, any such contribution becomes publicly available, subject to the relevant open source license. As a result, our ability to protect some of our intellectual property rights in such source code may be limited or lost entirely, and we would be unable to prevent our competitors or others from using such contributed source code in accordance with the relevant open source license.

Litigation may be necessary to enforce our intellectual property or proprietary rights, protect our trade secrets, or determine the validity and scope of proprietary rights claimed by others. Any litigation, whether or not resolved in our favor, could result in significant expense.

to us, divert the time and efforts of our technical and management personnel, and result in counterclaims alleging infringement of intellectual property rights by us or challenging the validity or scope of our intellectual property rights, which may lead to the impairment or loss of portions of our intellectual property. If we are unable to prevent third parties from infringing upon or misappropriating our intellectual property or are required to incur substantial expenses defending our intellectual property rights, our business, financial condition, and results of operations may be adversely affected.

If we are not successful in expanding our operations and customer base internationally, our business and results of operations could be negatively affected.

A component of our growth strategy involves the further expansion of our operations and customer base internationally. Customers outside the United States generated 30% and 31% of our total revenue for fiscal 2026 and 2025, respectively. We are continuing to adapt to and develop strategies to expand in international markets, but there is no guarantee that such efforts will have the desired effect. For example, we anticipate that we will need to establish relationships with new Channel Partners in order to expand into certain countries, and if we fail to identify, establish, and maintain such relationships, we may be unable to execute on our expansion plans. As of January 31, 2026, a substantial portion of our full-time employees were located outside of the United States. We expect that our international activities will continue to grow for the foreseeable future as we continue to pursue opportunities in existing and new international markets, which will require significant dedication of management attention and financial resources. If we invest substantial time and resources to further expand our international operations and are unable to do so successfully and in a timely manner, our business and results of operations will suffer.

We and the third parties with whom we work are subject to stringent and evolving U.S. and foreign laws, regulations, rules, contractual obligations, industry standards, policies, and other obligations relating to privacy and data security. Our (or the third parties with whom we work) actual or perceived failure to comply with such obligations could lead to heightened scrutiny by regulators, customers, investors, the media and the public, particularly with respect to sensitive data, AI-enabled functionality or security incident response. Any such actual or perceived failure could lead to regulatory investigations or actions, litigation (including class claims) and mass arbitration demands, fines and penalties, disruptions of our business operations, reputational harm, loss of revenue or profits, loss of customers or sales, and other adverse business consequences.

Due to the nature of the data security services and solutions we provide to our customers, we process various categories of sensitive information. Our data processing activities may subject us to numerous obligations relating to privacy and data security, such as various laws, regulations, guidance, industry standards, internal and external privacy and security policies, contractual requirements, and other obligations.

In the United States, federal, state, and local governments have enacted numerous data privacy and data security laws, including data breach notification laws, laws governing information about individuals, and consumer protection laws (e.g., Section 5 of the Federal Trade Commission Act) and other similar laws (e.g., wiretapping laws). For example, the federal Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), as amended by the Health Information Technology for Economic and Clinical Health Act (“HITECH”), imposes specific requirements relating to the privacy, security, and transmission of individually identifiable health information. Numerous U.S. states have enacted comprehensive privacy laws that impose certain obligations on covered businesses, including providing specific disclosures in privacy notices and affording residents with certain rights concerning their personal data. As applicable, such rights may include the right to access, correct, or delete certain personal data, and to opt-out of certain data processing activities, such as targeted advertising, profiling, and automated decision-making. The exercise of these rights may impact our business and ability to provide our products and services. Certain states also impose stricter requirements for processing certain personal data, including sensitive information, such as conducting data privacy impact assessments. These state laws allow for statutory fines for noncompliance. The California Consumer Privacy Act of 2018 (“CCPA”) applies to personal data of consumers, business representatives, and employees who are California residents, and requires businesses to provide specific disclosures in privacy notices and honor requests from such individuals to exercise certain privacy rights. The CCPA provides for fines and allows private litigants affected by certain data breaches to recover significant statutory damages. Similar laws are being considered in many other states as well as at the federal and local level, and we expect more states to pass similar laws in the future.

Outside the United States, an increasing number of laws, regulations, and industry standards may apply to our data processing activities. For example, the European Union’s General Data Protection Regulation (“EU GDPR”), the United Kingdom’s General Data Protection Regulation (“UK GDPR” and together with the EU GDPR, the “GDPR”), Australia’s Privacy Act, and the UAE’s Data Protection Law impose strict requirements for processing personal data and apply to our operations. Under the EU GDPR, companies may face temporary or definitive bans on data processing and other corrective actions, fines of up to 20 million Euros under the EU GDPR, 17.5 million pounds sterling under the UK GDPR or, in each case, 4% of annual global revenue, whichever is greater, or private litigation related to the processing of personal data brought by classes of data subjects or consumer protection organizations authorized

at law to represent their interests. Furthermore, in Europe, there is a proposed regulation related to AI that, if adopted, could impose onerous obligations related to the use of AI-related systems. In Canada, the Personal Information Protection and Electronic Documents Act ("PIPEDA"), and various related provincial laws, as well as Canada's Anti-Spam Legislation ("CASL"), may apply to our operations. We also have operations in Japan, India and Singapore and are subject to new and emerging data privacy regimes in Asia, including Japan's Act on the Protection of Personal Information, India's new privacy legislation, the Digital Personal Data Protection Act, and Singapore's Personal Data Protection Act.

Additionally, we may transfer personal data from Europe and other jurisdictions to the United States or other countries. Europe and other jurisdictions have enacted laws regulating the cross-border transfer of personal data from Europe to other countries, and, in particular, the European Economic Area and the United Kingdom, or UK, have significantly restricted the cross-border transfer of personal data to the United States, unless the entity has achieved compliance under the Data Privacy Framework and is listed as an active participant on the International Trade Administration's website. Currently, we are a listed participant. However, given historical challenges to similarly positioned frameworks, it is possible that the Data Privacy Framework may be invalidated in the future, and we will need to rely on other established transfer mechanisms for cross border transfers. Other jurisdictions may adopt similarly stringent interpretations of their cross-border data transfer laws. Although standard contractual clauses ("SCCs"), the UK's International Data Transfer Agreement / Addendum, and other mechanisms, currently may be used to transfer personal data from the European Economic Area to the United States, these mechanisms are frequently subject to legal challenges, and the efficacy and longevity of such mechanisms for making data transfers from the European Economic Area and the UK to the United States remains uncertain. If there is no lawful manner for us to transfer personal data from the European Economic Area and the UK or other jurisdictions to the United States, we could face significant consequences, including restricting our operations or relocating part of or all of our business to other jurisdictions and increased exposure to regulatory actions, substantial fines, civil proceedings, and injunctions against processing or transferring personal data, as well as incurring the associated legal and compliance costs. Some European regulators have ordered certain companies to suspend or permanently cease certain transfers of personal data out of Europe for allegedly violating the GDPR cross-border data transfer limitations.

We may also become subject to new laws that regulate non-personal information. For example, the European Union's Data Act imposes certain data and cloud service interoperability and switching obligations to enable users to switch between cloud service providers without undue delay or cost, as well as certain requirements concerning cross-border international transfers of, and governmental access to, non-personal information outside the European Economic Area. Depending on how this Act and any similar laws are implemented and interpreted, we may have to adapt our business practices, contractual arrangements, and services to comply with such obligations, which could impact our revenue and results of operations, if such changes impact our customers' subscription terms.

Additionally, the U.S. Department of Justice issued a rule entitled the Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, which places additional restriction on certain data transactions involving countries of concern (e.g., China, Russia, Iran) and covered persons that may impact certain business activities such as vendor engagements, sale or sharing of data, employment of certain individuals, and investor agreements. Violations of the rule could lead to significant civil and criminal fines and penalties.

In addition to privacy, data protection, and data security laws and regulations, we are and may in the future become contractually subject to industry standards adopted by industry groups, such as the Payment Card Industry Data Security Standards ("PCI"). Additionally, the demands our customers place on us relating to privacy, data protection, and data security are becoming more stringent. Data protection laws, such as the EU GDPR, UK GDPR, and CCPA, increasingly require companies to impose specific contractual restrictions on their service providers and contractors. In addition, customers that use certain of our solutions to process protected health information may require us to sign business associate agreements that subject us to the privacy and security requirements under HIPAA and HITECH, as well as state laws that govern the privacy and security of health information. Our customers' increasing data privacy and data security standards also increase the cost and complexity of ensuring that we, and the third parties we work with on to operate our business and deliver our services, can meet these standards. If we, or the third parties with whom we work, are unable to meet our customers' demands or comply with the increasingly stringent legal or contractual requirements relating to data privacy and data security, we may face increased legal liability, customer contract terminations, and reduced demand for our solutions.

Finally, we publish privacy policies, marketing materials, white papers and other statements, such as statements related to compliance with certain certifications or self-regulatory principles, as well as other documentation concerning data privacy, security, and AI. Regulators in the United States are increasingly scrutinizing these statements, and if these policies, materials, statements, or documentations are found to be deficient, lacking in transparency, deceptive, unfair, or misrepresentative of our practices, we may be subject to investigation, regulatory enforcement actions, costly legal claims by affected individuals or our customers, or other adverse consequences.

Obligations related to data privacy and data security (and consumers' data privacy expectations) are quickly changing, becoming increasingly stringent, and creating uncertainty. Additionally, these obligations may be subject to differing applications and interpretations by regulators and other stakeholders, which may be inconsistent or conflict among jurisdictions. Preparing for and complying with these obligations requires us to devote significant resources. These obligations may necessitate changes to our services, information technologies, systems, and practices and to those of any third parties that process personal data on our behalf. In addition, these obligations may require us to change our business model.

Our business model materially depends on our ability to process personal data, so we are particularly exposed to the risks associated with the rapidly changing legal landscape. We may be at heightened risk of regulatory scrutiny, and any changes in the regulatory framework could require us to fundamentally change our business model. Despite our efforts to comply with applicable data privacy and data security obligations, we may at times fail (or be perceived to have failed) in our efforts to comply. Moreover, despite our efforts, our personnel or third parties with whom we work may fail to comply with such obligations, which could negatively impact our business operations. If we, or the third parties with whom we work, fail, or are perceived to have failed, to address or comply with applicable data privacy and data security obligations, we could face significant consequences, including but not limited to: government enforcement actions (e.g., investigations, fines, penalties, audits, inspections, and similar); litigation (including class-action claims) and arbitration claims; additional reporting requirements and/or oversight; bans on processing personal data; orders to destroy or not use personal data; and imprisonment of company officials. As a data security company, we could be exposed to additional reputational risks should a data privacy incident occur. In particular, plaintiffs have become increasingly more active in bringing privacy-related claims against companies, including class claims and mass arbitration demands. Some of these claims allow for the recovery of statutory damages on a per violation basis, and, if viable, carry the potential for monumental statutory damages, depending on the volume of data and the number of violations.

As a result of being a public company, we are obligated to develop and maintain proper and effective internal controls over financial reporting, and any failure to maintain the adequacy of these internal controls may adversely affect investor confidence in our company and, as a result, the value of our Class A common stock.

We are required, pursuant to Section 404 of the Sarbanes-Oxley Act of 2002, as amended ("Sarbanes-Oxley Act"), to furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting. This assessment is required to include disclosure of any material weaknesses identified by our management in our internal control over financial reporting. In addition, our independent registered public accounting firm is required to attest to the effectiveness of our internal control over financial reporting. The process of compiling the system and process documentation necessary to perform the evaluation required under Section 404 of the Sarbanes-Oxley Act ("Section 404") is costly and challenging. Our compliance with Section 404 requires that we incur substantial expenses and expend significant management efforts. Although we currently have an internal audit group, we have in the past, and may in the future, need to hire additional accounting and financial staff with appropriate public company experience.

During the evaluation and testing process of our internal controls, if we identify one or more material weaknesses in our internal control over financial reporting, we will be unable to certify that our internal control over financial reporting is effective. We cannot assure you that there will not be material weaknesses or significant deficiencies in our internal control over financial reporting in the future. Any failure to maintain internal control over financial reporting could severely inhibit our ability to accurately report our financial condition or results of operations. If we are unable to conclude that our internal control over financial reporting is effective, or if our independent registered public accounting firm determines we have a material weakness or significant deficiency in our internal control over financial reporting, we could lose investor confidence in the accuracy and completeness of our financial reports, the market price of our Class A common stock could decline, and we could be subject to sanctions or investigations by the SEC or other regulatory authorities. Failure to remedy any material weakness in our internal control over financial reporting, or to implement or maintain other effective control systems required of public companies, could also restrict our future access to the capital markets.

We may become subject to intellectual property disputes, which can be costly and may subject us to significant liability and increased costs of doing business.

We have been and may continue in the future to be subject to intellectual property disputes. In regard to future litigation, our success depends, in part, on our ability to develop and commercialize our solutions without infringing, misappropriating, or otherwise violating the intellectual property rights of third parties. However, we may not be aware that our solutions are infringing, misappropriating, or otherwise violating third-party intellectual property rights, and such third parties may bring claims against us, our business partners, and our customers alleging such infringement, misappropriation, or violation. Companies in the software industry are often required to defend against litigation claims based on allegations of infringement, misappropriation, or other violations of intellectual property rights. For example, between 2020 and 2021, we were involved in patent disputes with two of our competitors which have since been resolved. However, we may not in all instances be able to obtain a settlement, or proactively defend or ascertain all third-party rights implicated by our business. Further, certain patent holders that own large numbers of patents and other intellectual property, including

“non-practicing entities,” often threaten or enter into litigation based on allegations of infringement or other violations of intellectual property rights. Any claims of intellectual property infringement, even those without merit, may be time-consuming and expensive to resolve, divert management’s time and attention, cause us to cease using or incorporating the challenged technology, expose us to other legal liabilities, such as indemnification obligations, or require us to enter into licensing agreements to obtain the right to use a third party’s intellectual property. In addition, many companies have the capability to dedicate substantially greater resources to enforce their intellectual property rights and to defend claims that may be brought against them. Any litigation may also involve patent holding companies or other adverse patent owners that have no relevant product revenue, and therefore, our patents may provide little or no deterrence as we would not be able to assert them against such entities or individuals. If we are found to infringe a third-party’s intellectual property rights and we cannot obtain a license or develop a non-infringing alternative, we would be forced to cease business activities related to such intellectual property. Although we carry general liability insurance, our insurance may not cover potential claims of this type or may not be adequate to indemnify us for all liability that may be imposed. We cannot predict the outcome of lawsuits and cannot ensure that the results of any such actions will not have an adverse effect on our business, financial condition, or results of operations. Any intellectual property litigation to which we might become a party, or for which we are required to provide indemnification, may require us to do one or more of the following:

- cease selling or using solutions that incorporate the intellectual property rights that we allegedly infringe, misappropriate, or violate;
- make substantial payments for legal fees, settlement payments, or other costs or damages;
- obtain a license, which may not be available on reasonable terms or at all, to sell or use the relevant technology; or
- redesign the allegedly infringing solutions to avoid infringement, misappropriation, or violation, which could be costly, time-consuming, or impossible.

Even if the claims do not result in litigation or are resolved in our favor, these claims, and the time and resources necessary to resolve them, could divert the resources of our management and harm our business and results of operations. Moreover, there could be public announcements of the results of hearings, motions or other interim proceedings or developments, and if securities analysts or investors perceive these results to be negative, it could have a substantial adverse effect on the price of our Class A common stock. We expect that the occurrence of infringement claims is likely to grow as our business grows. Accordingly, our exposure to damages resulting from infringement claims could increase, and this could further exhaust our financial and management resources.

We and our employees have and may continue to be subject to claims alleging violations of our employees’ contractual obligations to their prior employers. These claims may be costly to defend, and if we do not successfully do so, our business could be harmed.

Many of our employees were previously employed at current or potential competitors. Although we have processes to ensure that our employees do not use proprietary information or disclose confidential information from their prior employer in their work for us or otherwise violate their contractual post-employment obligations such as customer and employee non-solicits, we or our employees have in the past been, and may in the future, be subject to claims alleging such violations. Litigation has been, and may in the future be, necessary to defend against these claims and we have not always been successful in defending these claims. If we fail in defending such claims, in addition to paying monetary damages, we may lose valuable intellectual property rights or personnel. A loss of key personnel or their work product could negatively impact our business. Even if we are successful in defending against these claims, litigation efforts are costly, time-consuming, and a significant distraction to management.

Our company values have contributed to our success. If we cannot maintain these values as we grow, we could lose certain benefits we derive from them, and our employee turnover could increase, which could harm our business.

We believe our culture is driven by our company values which have been and will continue to be a key contributor to our success. Our core company values are:

- **Relentlessness.** Unyielding will and curiosity to tackle the hardest challenges.
- **Integrity.** Do what you say and do the right thing.
- **Velocity.** Drive clarity, decide quickly, and move fast to delight our customers.
- **Excellence.** Set a high standard and strive for greatness.
- **Transparency.** Build trust and drive smart decisions through transparent communication.

We have rapidly increased our workforce across all departments, and we expect to continue to hire across our business. Our anticipated headcount growth may result in changes to certain employees’ adherence to our core company values. If we do not continue to maintain our adherence to our company values as we grow, including through any future acquisitions or other strategic transactions, we may experience increased turnover in a portion of our current employee base and may not continue to be successful in

hiring future employees. Moreover, many of our employees may be eligible to receive significant proceeds from the sale of Class A common stock in the public markets. This may lead to higher employee attrition rates or disparities in wealth among our employees, which may harm our culture and relations among employees.

We are subject to risks inherent in international operations that can harm our business, financial condition, and results of operations.

Our current and future international business and operations involve a variety of risks, including:

- slower than anticipated availability and adoption of cloud-based solutions by international organizations;
- changes in a specific country's or region's political or economic conditions;
- the need to adapt and localize our solutions for specific countries;
- greater difficulty collecting accounts receivable and longer payment cycles;
- potential changes in trade relations, regulations, or laws;
- unexpected changes in laws, including tax laws, or regulatory requirements;
- more stringent regulations relating to privacy, data security, and data localization requirements and the unauthorized use of, or access to, commercial and personal information;
- differing and potentially more onerous labor regulations, especially in Europe, where labor laws are generally more advantageous to employees as compared to the United States, including deemed hourly wage and overtime regulations in these locations;
- challenges inherent in efficiently managing, and the increased costs associated with, an increased number of employees over large geographic distances, including the need to implement appropriate systems, policies, benefits, and compliance programs that are specific to each jurisdiction;
- difficulties in managing a business in new markets with diverse cultures, languages, customs, legal systems, alternative dispute systems, and regulatory systems;
- increased travel, real estate, infrastructure, and legal compliance costs associated with international operations;
- currency exchange rate fluctuations and the resulting effect on our revenue and expenses, and the cost and risk of entering into hedging transactions if we choose to do so in the future;
- limitations on our ability to reinvest earnings from operations in one country to fund the capital needs of our operations in other countries;
- laws and business practices favoring local competitors or general market preferences for local vendors;
- limited or insufficient intellectual property protection or difficulties obtaining, maintaining, protecting, or enforcing our intellectual property rights, including our trademarks and patents, in the United States or other foreign jurisdictions;
- political instability, economic sanctions, terrorist activities, or international conflicts, including the conflict in Israel and Middle East and the ongoing conflict between Russia and Ukraine, which have in the past and may in the future impact the operations of our business or the businesses of our customers;
- inflationary pressures, such as those the global market is currently experiencing, which may increase costs for certain services;
- health epidemics or pandemics;
- exposure to liabilities under anti-corruption and similar laws, including FCPA, U.S. domestic bribery laws, the UK Bribery Act, and similar laws and regulations in other jurisdictions; and
- adverse tax burdens and foreign exchange controls that could make it difficult to repatriate earnings and cash.

The occurrence of any one of these risks could harm our international business and, consequently, our results of operations. Additionally, operating in international markets requires significant management attention and financial resources. We cannot be certain that the investment and additional resources required to operate in other countries will produce desired levels of revenue or profitability.

Changes in tax laws or regulations could harm our financial condition and results of operations.

The tax regimes to which we are subject or under which we operate, including income and non-income taxes, are unsettled in certain respects and may be subject to significant change. Changes in tax laws or regulations, or changes in interpretations of existing laws and regulations, could materially affect our financial condition and results of operations. Legislation commonly referred to as the One Big Beautiful Bill Act (the "OBBBA"), as well as the Tax Cuts and Jobs Act (the "Tax Act"), the Coronavirus Aid, Relief, and Economic Security Act, and the Inflation Reduction Act made many significant changes to the U.S. tax laws. For example, for tax years beginning after December 31, 2024, the OBBBA restores the deductibility of domestic research and development expenses in the year incurred,

which expenses had been required under the Tax Act to be capitalized and subsequently amortized over five years. The OBBBA did not change the tax treatment of expenses incurred in research and development activities conducted outside the United States, which expenses continue to be required to be capitalized and amortized over 15 years. The Tax Act also includes certain U.S. tax base anti-erosion provisions, the global intangible low-taxed income ("GILTI") provisions, and the base erosion anti-abuse tax ("BEAT") provisions. The GILTI provisions require us to include in our U.S. taxable income foreign subsidiary earnings in excess of an allowable return on the foreign subsidiary's tangible assets. The OBBBA modified the GILTI provisions to refer to net CFC tested income ("NCTI"), eliminate the allowable return on the foreign subsidiary's tangible assets for taxable years beginning after December 31, 2025, and increase but make permanent the effective tax rate on NCTI. We currently have no foreign subsidiaries with material earnings. Therefore, this provision currently has no material impact on us. The BEAT provisions apply to companies with average annual gross receipts of \$500 million or more for the prior three-year period, eliminate the deduction of certain base-erosion payments made to related foreign corporations, and impose a minimum tax if greater than regular tax. We are evaluating the BEAT rules and do not currently expect the BEAT rules to have a material impact on U.S. tax expense in the near term; however, the potential impact of the BEAT rules on us in the future is not certain.

In addition, our tax obligations (including the cost of compliance) and effective tax rate in the jurisdictions in which we conduct business could increase, including as a result of the base erosion and profit shifting ("BEPS") project that is being led by the Organization for Economic Co-operation and Development ("OECD"), and other initiatives led by the OECD or the European Commission. For example, the OECD is leading work on proposals commonly referred to as "BEPS 2.0," which have made (and are expected to continue to make) important changes to the international tax system. These proposals are based on two "pillars," involving, among other measures, the imposition of a minimum effective tax rate on certain multinational enterprises, referred to as "Pillar Two." A number of countries in which we conduct business have enacted, or are in the process of enacting, core elements of the Pillar Two rules (with further provisions expected to be enacted in the future). Based on our current understanding of the minimum revenue thresholds contained in the Pillar Two proposal, we will fall within the scope of its rules in our fiscal year ending January 31, 2027. The OECD has issued (and is expected to continue to issue further) administrative guidance providing transition and safe harbor rules in relation to the implementation of the Pillar Two proposal. For example, on January 5, 2026, the OECD published details of a proposed "side-by-side" arrangement providing for, among other things, additional safe harbors for multinational groups headquartered in certain qualifying jurisdictions. We are monitoring developments and evaluating the potential impacts of Pillar Two rules, including on our effective tax rates, and considering our eligibility to qualify for these safe harbor rules (including under the proposed "side-by-side" arrangement). As another example, several countries have proposed or enacted taxes applicable to digital services, which could apply to our business.

Due to the large and expanding scale of our international business activities, these types of changes to the taxation of our activities could increase our worldwide effective tax rate, increase the amount of taxes imposed on our business, and increase our compliance costs. Such changes also may apply retroactively to our historical operations and result in taxes greater than the amounts estimated and recorded in our unaudited condensed consolidated financial statements. Any of these outcomes could harm our financial position and results of operations.

We could be required to collect additional sales or other indirect taxes or be subject to other tax liabilities in various jurisdictions that may adversely affect our results of operations.

We sell subscriptions and services primarily through a distribution channel, but if we were to begin selling more (or, in respect of certain jurisdictions, any) subscriptions and services directly to end user or non-business customers, we may be adversely impacted because an increasing number of U.S. states and foreign jurisdictions have adopted laws that impose tax collection obligations on out-of-state companies or on companies with no taxable presence within such jurisdictions other than economic nexus. State, local, or foreign governments may interpret existing laws, or adopt new laws, requiring us to calculate, collect and remit taxes on sales in their jurisdictions. A successful assertion by one or more taxing jurisdictions requiring us to collect taxes in jurisdictions in which we do not currently do so or to collect additional taxes in jurisdictions in which we currently collect taxes, could result in substantial tax liabilities, including taxes on past sales, as well as penalties and interest, and additional administrative expenses, which could harm our business. The imposition by state, local, or foreign governments of sales or other indirect tax collection obligations on out-of-state sellers or sellers with no taxable presence within the relevant jurisdiction other than economic nexus also could create additional administrative burdens for us, put us at a competitive disadvantage if they do not impose similar obligations on our competitors, and decrease our future sales, which could have an adverse effect on our business and results of operations.

Our ability to use our net operating losses to offset future taxable income may be subject to certain limitations.

As of January 31, 2026, we had net operating loss ("NOL") carryforwards for federal and state income tax purposes of \$1.97 billion and \$870.7 million, respectively, which may be available to offset taxable income in the future, and portions of which expire in various years beginning in 2037 for federal purposes and 2027 for state purposes if not utilized. U.S. federal NOLs incurred in taxable years beginning after December 31, 2017 may be carried forward indefinitely, but such federal NOL carryforwards are permitted to be used in

any taxable year to offset only up to 80% of taxable income in such year. A lack of future taxable income would adversely affect our ability to utilize certain of these NOL carryforwards before they expire. In addition, under Section 382 of the Internal Revenue Code of 1986, as amended (the "Code"), a corporation that undergoes an "ownership change" (as defined under Section 382 of the Code and applicable Treasury Regulations; generally a greater than 50 percentage point change (by value) in its equity ownership by certain stockholders over a three-year period) is subject to limitations on its ability to utilize its pre-change NOL carryforwards to offset future taxable income. We have experienced an ownership change under Section 382 of the Code in the past and we may experience additional ownership changes in the future which could affect our ability to utilize our NOL carryforwards to offset our income. Similar provisions of state tax law may also apply. Furthermore, our ability to utilize NOLs of companies that we have acquired or may acquire in the future also may be subject to limitations. There is also a risk that due to regulatory changes, such as suspensions on the use of NOLs or other unforeseen reasons, our existing NOLs could expire or otherwise be unavailable to reduce future income tax liabilities, including for state tax purposes. For example, California has suspended the use of California state net operating losses to offset taxable income in tax years beginning after 2023 and before 2027. For these reasons, we may not be able to utilize a material portion of the NOLs reflected on our balance sheet, even if we attain profitability, which could potentially result in increased future tax liability to us and could adversely affect our results of operations and financial condition.

We may be subject to additional tax liabilities, which could adversely affect our results of operations.

We are subject to taxes in the United States in federal, state, and local jurisdictions and in certain foreign jurisdictions in which we operate. The amount of taxes we pay in different jurisdictions depends on the application of the relevant tax laws to our business activities, the relative amounts of income before taxes in the various jurisdictions in which we operate, the application of new or revised tax laws, the interpretation of existing tax laws and policies, the outcome of current and future tax audits, examinations, or administrative appeals, our ability to realize our deferred tax assets, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements. We generally conduct our international operations through subsidiaries and report our taxable income in various jurisdictions worldwide based upon our business operations in those jurisdictions. Our intercompany relationships are subject to complex transfer pricing regulations administered by taxing authorities in various jurisdictions. We may be subject to examination by U.S. federal, state, local, and foreign tax authorities, and such tax authorities may disagree with our tax positions. Our methodologies for pricing intercompany transactions may be challenged, or the taxing authorities in the jurisdictions in which we operate may disagree with our determinations as to the income and expenses attributable to specific jurisdictions or the ownership of certain property acquired or developed pursuant to our intercompany arrangements or property of companies that we have acquired or may acquire in the future. If such a challenge or disagreement were to occur and our position was not sustained, we could be required to pay additional taxes, interest, and penalties, which could result in one-time tax charges, higher effective tax rates, reduced cash flows, and lower overall profitability of our operations. While we regularly assess the likelihood of adverse outcomes from any such examinations and the adequacy of our provision for taxes, there can be no assurance that such provision is sufficient or that a determination by a tax authority would not adversely affect our business, financial condition, and results of operations. The determination of our overall provision for income and other taxes is inherently uncertain because it requires significant judgment with respect to complex transactions and calculations. As a result, fluctuations in our tax liabilities may differ materially from amounts recorded in our financial statements and could adversely affect our business, financial condition, and results of operations in the periods for which such determination is made.

If our estimates or judgments relating to our critical accounting policies prove to be incorrect, our results of operations could be adversely affected.

The preparation of financial statements in conformity with GAAP requires management to make estimates and assumptions that affect the amounts reported in our unaudited condensed consolidated financial statements and accompanying notes appearing elsewhere in this Quarterly Report on Form 10-Q. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as provided in the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations—Critical Accounting Policies and Estimates." The results of these estimates form the basis for making judgments about the carrying values of assets, liabilities and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant estimates and judgments involve our common stock valuations prior to the completion of the IPO, the volatility used to determine the grant date fair value of the performance option grant for our CEO, the identification of the number of performance obligations in our RSC subscription offerings, and our material rights associated with Subscription Credits. Our results of operations may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our results of operations to fall below the expectations of securities analysts and investors, resulting in a decline in the market price of our Class A common stock.

Our leverage could adversely affect our financial condition, our ability to raise additional capital to fund our operations, our ability to operate our business, and our ability to react to changes in the economy or our industry, as well as divert our cash flow from operations for debt payments and prevent us from meeting our debt obligations.

We issued \$1.15 billion of the Notes in June 2025 pursuant to the Indenture. We previously entered into the Amended Credit Facility in August 2023 with Goldman Sachs BDC, Inc., as administrative agent, and the other lenders party thereto, consisting of a \$289.5 million term loan and \$40.5 million of committed delayed draw term loans. In June 2025, we used a portion of the net proceeds from the issuance of the Notes to repay all outstanding balance of \$327.9 million under the Amended Credit Facility, and also terminated the Amended Credit Facility.

Our leverage could have an adverse effect on our business and financial condition, including:

- requiring a substantial portion of cash flow from operations to be dedicated to the payment of principal and interest on our indebtedness, thereby reducing our ability to use our cash flow to fund our operations and capital expenditures and pursue future business opportunities;
- exposing us to increased interest expense, as our degree of leverage may cause the interest rates of any future indebtedness, whether fixed or floating rate interest, to be higher than they would be otherwise;
- making it more difficult for us to satisfy our obligations with respect to our indebtedness, and any failure to comply with the obligations of any of our debt instruments, including restrictive covenants, could result in an event of default that accelerates our obligation to repay indebtedness;
- restricting us from making strategic acquisitions;
- limiting our ability to obtain additional financing for working capital, capital expenditures, product development, satisfaction of debt service requirements, acquisitions, and general corporate or other purposes;
- increasing our vulnerability to adverse economic, industry, or competitive developments; and
- limiting our flexibility in planning for, or reacting to, changes in our business or market conditions and placing us at a competitive disadvantage compared to our competitors who may be better positioned to take advantage of opportunities that our existing indebtedness prevents us from exploiting.

We now have, and may continue to have, debt obligations. A substantial majority of our existing indebtedness consists of indebtedness under the Notes, which matures in June 2030. We may not be able to further refinance the existing indebtedness because of the amount of our debt or adverse conditions in credit markets generally. Our inability to generate sufficient cash flow to satisfy our obligations, or to refinance our indebtedness on commercially reasonable terms or at all, would result in an adverse effect on our business, financial condition, and results of operations.

Furthermore, we may incur significant additional indebtedness in the future. Additional indebtedness incurred in the future could be substantial. To the extent we incur additional indebtedness, the significant leverage risks described above would be exacerbated.

Risks Related to Ownership of Our Common Stock

The dual class structure of our common stock has the effect of concentrating voting control with the holders of our Class B common stock, including our executive officers, employees, and directors and their affiliates, and limiting your ability to influence corporate matters, which could adversely affect the trading price of our Class A common stock.

Our Class B common stock has 20 votes per share, whereas our Class A common stock has one vote per share. As a result, as of April 30, 2026, holders of our Class B common stock, including our executive officers and directors and their affiliates, together hold approximately 85% of the voting power of our outstanding capital stock, and our directors, executive officers, and affiliated stockholders beneficially own approximately 22% of our outstanding classes of common stock as a whole, but control approximately 81% of the voting power of our outstanding common stock. As a result, our executive officers, directors, and other affiliates have significant influence over our management and affairs and over all matters requiring stockholder approval, including election of directors and significant corporate transactions, such as a merger or other sale of the company or our assets, for the foreseeable future.

In addition, the holders of Class B common stock collectively will continue to be able to control all matters submitted to our stockholders for approval even if their stock holdings represent less than 50% of the outstanding shares of our common stock. Because of the 20-to-1 voting ratio between our Class B common stock and Class A common stock, the holders of our Class B common stock collectively will continue to control a majority of the combined voting power of our common stock even when the shares of Class B common stock represent as little as 5% of the outstanding shares of our Class A common stock and Class B common stock. This concentrated control will limit your ability to influence corporate matters for the foreseeable future, and, as a result, the market price of our Class A common stock could be adversely affected.

Future transfers by holders of shares of Class B common stock will generally result in those shares converting to shares of Class A common stock, which will have the effect, over time, of increasing the relative voting power of those holders of Class B common stock who retain their shares in the long term.

FTSE Russell does not allow most newly public companies utilizing dual or multi-class capital structures to be included in their indices, including the Russell 2000. Also, in 2017, MSCI, a leading stock index provider, opened public consultations on its treatment of no-vote and multi-class structures and temporarily barred new multi-class listings from certain of its indices; however, in October 2018, MSCI announced its decision to include equity securities “with unequal voting structures” in its indices and to launch a new index that specifically includes voting rights in its eligibility criteria. Under the announced policies, our dual class capital structure would make us ineligible for inclusion in certain indices, and as a result, mutual funds, exchange-traded funds, and other investment vehicles that attempt to passively track these indices will not be investing in our stock. In addition, we cannot assure you that other stock indices will not take similar actions. Given the sustained flow of investment funds into passive strategies that seek to track certain indices, exclusion from certain stock indices would likely preclude investment by many of these funds and would make our Class A common stock less attractive to other investors. As a result, the trading price, volume, and liquidity of our Class A common stock could be adversely affected.

Our stock price may be volatile, and the value of our Class A common stock may decline.

The market price of our Class A common stock may be highly volatile and may fluctuate or decline substantially as a result of a variety of factors, some of which are beyond our control, including:

- actual or anticipated fluctuations in our financial condition or results of operations;
- variance in our financial performance from our forecasts or the expectations of securities analysts;
- changes in our revenue mix;
- changes in the pricing of our solutions;
- changes in our projected operating and financial results;
- changes in laws or regulations applicable to our solutions;
- announcements by us or our competitors of significant business developments, acquisitions, or new solutions;
- significant data breaches, disruptions to, or other incidents involving our data security solutions;
- our involvement in litigation;
- future sales of our Class A common stock by us or our stockholders;
- changes in senior management or key personnel;
- the trading volume of our Class A common stock;
- changes in the anticipated future size and growth rate of our market;
- changes in demand for cybersecurity offerings;
- rumors and market speculation involving us or other companies in our industry;
- investor sentiment regarding AI-related business models, our competitors, and our industry in general;
- overall performance of the equity markets;
- general political, social, economic, and market conditions, in both domestic and our foreign markets, including effects of increased; and
- interest rates, inflationary pressures, bank failures, and macroeconomic uncertainty and challenges.

Broad market and industry fluctuations, as well as general economic, political, regulatory, and market conditions, may also negatively impact the market price of our Class A common stock. In addition, technology stocks have historically experienced high levels of volatility. In the past, companies that have experienced volatility in the market price of their securities have been subject to securities class action litigation. We may be the target of this type of litigation in the future, which could result in substantial expenses and divert our management’s attention.

Future sales of our Class A common stock in the public market could cause the market price of our Class A common stock to decline.

Sales of a substantial number of shares of our Class A common stock in the public market following our IPO, or the perception that these sales might occur, could depress the market price of our Class A common stock and could impair our ability to raise capital through the sale of additional equity securities. Many of our equity holders have substantial unrecognized gains on the value of the equity they hold, and therefore, they may take steps to sell their shares or otherwise secure the unrecognized gains on those shares.

We are unable to predict the timing of or the effect that such sales may have on the prevailing market price of our Class A common stock.

In addition, as of April 30, 2026, there were 8,817,693 shares of Class B common stock issuable upon the exercise of options and 6,199,676 restricted stock units ("RSUs"), to be settled in shares of our Class B common stock. We have registered all of the shares of Class A common stock issuable upon exercise of outstanding options, the vesting and settlement of outstanding RSUs, and other equity incentives we may grant in the future, for public resale under the Securities Act. The shares of Class A common stock will become eligible for sale in the public market to the extent such options are exercised or RSUs are vested and settled, subject to compliance with applicable securities laws.

Further, certain holders of our common stock have rights, subject to some conditions, to require us to file registration statements covering the sale of their shares or to include their shares in registration statements that we may file for ourselves or other stockholders.

The capped call transactions may affect the market price of the Notes and our Class A common stock.

In connection with the pricing of the Notes and the exercise in full by the initial purchasers of their option to purchase additional Notes, we entered into capped call transactions with certain affiliates of certain initial purchasers and other financial institutions (the "option counterparties"). The capped call transactions cover, subject to anti-dilution adjustments substantially similar to those applicable to the Notes, the number of shares of our Class A common stock initially underlying the Notes. The capped call transactions are expected generally to reduce the potential dilution to our Class A common stock upon any conversion of the Notes and/or offset any cash payments we are required to make in excess of the principal amount of converted Notes, as the case may be, with such reduction and/or offset subject to a cap.

In connection with establishing their initial hedges of the capped call transactions, the option counterparties or their respective affiliates entered into various derivative transactions with respect to our Class A common stock and/or purchased shares of our Class A common stock concurrently with or shortly after the pricing of the Notes, including with, or from, as the case may be, certain investors in the Notes. This activity could increase (or reduce the size of any decrease in) the market price of our Class A common stock.

In addition, the option counterparties or their respective affiliates may modify their hedge positions by entering into or unwinding various derivatives with respect to our Class A common stock and/or purchasing or selling our Class A common stock or other securities of ours in secondary market transactions following the pricing of the Notes and prior to the maturity of the Notes (and are likely to do so following any conversion, repurchase upon a fundamental change or redemption of the Notes, or, to the extent we exercise the relevant election under the capped call transactions, following any other repurchase of the Notes). This activity could also cause or avoid an increase or a decrease in the market price of our Class A common stock or the Notes.

We are subject to counterparty risk with respect to the capped call transactions.

The option counterparties are financial institutions, and we will be subject to the risk that any or all of them might default under the capped call transactions. Our exposure to the credit risk of the option counterparties will not be secured by any collateral.

Global economic conditions have from time to time resulted in the actual or perceived failure or financial difficulties of many financial institutions and could adversely affect the option counterparties' performance under the capped call transactions. If an option counterparty becomes subject to insolvency proceedings, we will become an unsecured creditor in those proceedings with a claim equal to our exposure at that time under the capped call transactions with such option counterparty. Our exposure will depend on many factors but, generally, an increase in our exposure will be correlated to an increase in the market price and in the volatility of our Class A common stock. In addition, upon a default by an option counterparty, we may suffer more dilution, than we currently anticipate with respect to our Class A common stock. We can provide no assurance as to the financial stability or viability of the option counterparties.

Our issuance of additional capital stock in connection with financings, acquisitions, investments, our equity incentive plans, or otherwise, or the conversion or exercise of certain of our securities will dilute all other stockholders.

We expect to issue additional capital stock in the future that will result in dilution to all other stockholders. We expect to grant equity awards to employees, directors, and consultants under our equity incentive plans. We may also raise capital through equity financings in the future. As part of our business strategy, we may acquire or make investments in companies, products, or technologies and issue equity securities to pay for any such acquisition or investment. In addition, the conversion of some or all of the Notes may dilute the ownership interests of our stockholders. Upon conversion of the Notes, we have the option to pay or deliver, as the case may be, cash, shares of our Class A common stock, or a combination of cash and shares of our Class A common stock. If we elect to settle our conversion obligation in shares of our Class A common stock or a combination of cash and shares of our common stock with respect to conversions of the Notes, any sales in the public market of our Class A common stock issuable upon such conversion could adversely

affect prevailing market prices of our Class A common stock. Any such issuances of additional capital stock may cause stockholders to experience significant dilution of their ownership interests and the per share value of our Class A common stock to decline.

We do not intend to pay dividends for the foreseeable future and, as a result, your ability to achieve a return on your investment will depend on appreciation in the price of our Class A common stock.

We have never declared or paid any cash dividends on our capital stock, and we do not intend to pay any cash dividends in the foreseeable future. Any determination to pay dividends in the future will be at the discretion of our board of directors. Additionally, our ability to pay dividends may be further restricted by agreements we may enter into in the future. Accordingly, you may need to rely on sales of our Class A common stock after price appreciation, which may never occur, as the only way to realize any future gains on your investment.

We incur significant costs as a result of operating as a public company, and our management is required to devote substantial time to compliance with our public company responsibilities and corporate governance practices.

As a public company, we incur significant legal, accounting, and other expenses that we did not incur as a private company. We expect such expenses to further increase now that we are a large accelerated filer. The Sarbanes-Oxley Act, the Dodd-Frank Wall Street Reform and Consumer Protection Act, the listing requirements of the New York Stock Exchange, and other applicable securities rules and regulations impose various requirements on public companies. Our management and other personnel devote a substantial amount of time to compliance with these requirements. Moreover, these rules and regulations have increased our legal and financial compliance costs and have made some activities more time-consuming and costly. We cannot predict or estimate the amount of additional costs we will incur as a public company or the specific timing of such costs.

Anti-takeover provisions in our charter documents, the Indenture, and under Delaware law could make an acquisition of our company more difficult, limit attempts by our stockholders to replace or remove our current management, and limit the market price of our Class A common stock.

Provisions in our amended and restated certificate of incorporation and amended and restated bylaws may have the effect of preventing a change of control or changes in our management. Our amended and restated certificate of incorporation and amended and restated bylaws include provisions that:

- authorize our board of directors to issue, without further action by the stockholders, shares of undesignated preferred stock with terms, rights, and preferences determined by our board of directors that may be senior to our Class A common stock;
- require that any action to be taken by our stockholders be effected at a duly called annual or special meeting and not by written consent;
- specify that special meetings of our stockholders can be called only by our board of directors, the chairperson of our board of directors, our chief executive officer, or our president (in the absence of a chief executive officer);
- establish an advance notice procedure for stockholder proposals to be brought before an annual meeting, including proposed nominations of persons for election to our board of directors;
- establish that our board of directors is divided into three classes, with each class serving three-year staggered terms;
- prohibit cumulative voting in the election of directors;
- provide that our directors may be removed for cause only upon the vote of at least 66 2/3% of our outstanding shares of voting stock;
- provide that vacancies on our board of directors may be filled only by the affirmative vote of a majority of directors then in office, even though less than a quorum, or by a sole remaining director; and
- require the approval of our board of directors or the holders of at least 66 2/3% of our outstanding shares of voting stock to amend our bylaws and certain provisions of our certificate of incorporation.

These provisions may frustrate or prevent any attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors, which is responsible for appointing the members of our management. In addition, because we are incorporated in Delaware, we are governed by the provisions of Section 203 of the Delaware General Corporation Law, which generally, subject to certain exceptions, prohibits a Delaware corporation from engaging in any of a broad range of business combinations with any “interested” stockholder for a period of three years following the date on which the stockholder became an “interested” stockholder. Any of the foregoing provisions could limit the price that investors might be willing to pay in the future for shares of our Class A common stock, and they could deter potential acquirers of our company, thereby reducing the likelihood that holders of our Class A common stock would receive a premium for their shares of our Class A common stock in an acquisition.

In addition, certain provisions in the Indenture may make it more difficult or expensive for a third party to acquire us. For example, the Indenture will require us, except as described therein, to repurchase the Notes for cash upon the occurrence of a fundamental change and, in certain circumstances, to increase the conversion rate for a holder that converts its Note in connection with a make-whole fundamental change (as defined in the Indenture). A takeover of us may trigger the requirement that we repurchase the Notes and/or increase the conversion rate, which could make it costlier for a potential acquirer to engage in such takeover. Such additional costs may have the effect of delaying or preventing a takeover of us that would otherwise be beneficial to investors.

Our amended and restated certificate of incorporation designates the Court of Chancery of the State of Delaware and the federal district courts of the United States of America as the exclusive forums for certain disputes between us and our stockholders, which restricts our stockholders' ability to choose the judicial forum for disputes with us or our directors, officers, or employees.

Our amended and restated certificate of incorporation provides that the Court of Chancery of the State of Delaware (or, if and only if the Court of Chancery of the State of Delaware lacks subject matter jurisdiction, any state court located within the State of Delaware or, if and only if all such state courts lack subject matter jurisdiction, the federal district court for the District of Delaware) is the sole and exclusive forum for the following types of actions or proceedings under Delaware statutory or common law: (i) any derivative action or proceeding brought on our behalf; (ii) any action or proceeding asserting a claim of breach of a fiduciary duty owed by any of our current or former directors, officers, or other employees to us or our stockholders, or any action asserting a claim for aiding and abetting such breach of fiduciary duty; (iii) any action or proceeding asserting a claim against us or any of our current or former directors, officers or other employees arising out of or pursuant to any provision of the Delaware General Corporation Law, our amended and restated certificate of incorporation or our amended and restated bylaws; (iv) any action or proceeding to interpret, apply, enforce or determine the validity of our amended and restated certificate of incorporation or our amended and restated bylaws (including any right, obligation, or remedy thereunder); (v) any action or proceeding as to which the Delaware General Corporation Law confers jurisdiction to the Court of Chancery of the State of Delaware; and (vi) any action or proceeding asserting a claim against us or any of our current or former directors, officers, or other employees that is governed by the internal affairs doctrine, in all cases to the fullest extent permitted by law and subject to the court's having personal jurisdiction over the indispensable parties named as defendants. This provision does not apply to suits brought to enforce a duty or liability created by the Exchange Act, or any other claim for which the federal courts have exclusive jurisdiction. In addition, to prevent having to litigate claims in multiple jurisdictions and the threat of inconsistent or contrary rulings by different courts, among other considerations, our amended and restated certificate of incorporation provides that, unless we consent in writing to the selection of an alternative forum, to the fullest extent permitted by law, the federal district courts of the United States of America are the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act, including all causes of action asserted against any defendant named in such complaint. For the avoidance of doubt, this provision is intended to benefit and may be enforced by us, our officers and directors, the underwriters to any offering giving rise to such complaint, and any other professional entity whose profession gives authority to a statement made by that person or entity and who has prepared or certified any part of the documents underlying the offering. However, as Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over all suits brought to enforce any duty or liability created by the Securities Act or the rules and regulations thereunder, there is uncertainty as to whether a court would enforce such provision. Our amended and restated certificate of incorporation further provides that any person or entity holding, owning, or otherwise acquiring any interest in any of our securities shall be deemed to have notice of and consented to these provisions. Investors also cannot waive compliance with the federal securities laws and the rules and regulations thereunder.

These choice of forum provisions may limit a stockholder's ability to bring a claim in a judicial forum that it finds favorable for disputes with us or our directors, officers, or other employees. While the Delaware courts have determined that such choice of forum provisions are facially valid, a stockholder may nevertheless seek to bring such a claim arising under the Securities Act against us, our directors, officers, or other employees in a venue other than in the federal district courts of the United States of America. In such instance, we would expect to vigorously assert the validity and enforceability of the exclusive forum provisions of our amended and restated certificate of incorporation. This may require significant additional costs associated with resolving such action in other jurisdictions and we cannot assure you that the provisions will be enforced by a court in those other jurisdictions. If a court were to find either exclusive-forum provision in our amended and restated certificate of incorporation to be inapplicable or unenforceable in an action, we may incur further significant additional costs associated with resolving the dispute in other jurisdictions, all of which could harm our business.

If securities or industry analysts do not publish research or publish unfavorable or inaccurate research about our business, the market price and trading volume of our Class A common stock could decline.

The market price and trading volume of our Class A common stock is heavily influenced by the way analysts interpret our financial information and other disclosures. We do not have control over these analysts. If industry analysts cease coverage of us, our stock price would be negatively affected. If securities or industry analysts do not publish research or reports about our business, downgrade our Class A common stock, or publish negative reports about our business, our stock price would likely decline. If one or more of these

analysts cease coverage of us or fail to publish reports on us regularly, demand for our Class A common stock could decrease, which might cause our stock price to decline and could decrease the trading volume of our Class A common stock.

General Risk Factors

Any future litigation against us could be costly and time-consuming to defend.

We have in the past been and in the future may become subject to legal proceedings and claims that arise in the ordinary course of business, such as intellectual property claims, including trade secret misappropriation and breaches of confidentiality terms, alleged breaches of non-competition or non-solicitation terms, or employment claims made by our current or former employees. Litigation might result in substantial costs and may divert management's attention and resources, which might seriously harm our business, financial condition, and results of operations. Insurance might not cover such claims, might not provide sufficient payments to cover all the costs to resolve one or more such claims, and might not continue to be available on terms acceptable to us. A claim brought against us that is uninsured or underinsured could result in unanticipated costs, potentially harming our business, financial condition, and results of operations.

Our business could be disrupted by catastrophic events.

Occurrence of any catastrophic event, including earthquake, fire, flood, tsunami, or other weather event, power loss, telecommunications failure, software or commodity appliance malfunction, cyberattack, war, or terrorist attack, explosion, or pandemic could impact our business. In particular, our corporate headquarters are located in the San Francisco Bay Area, a region known for seismic activity, and are thus vulnerable to damage in an earthquake. Our insurance coverage may not compensate us for losses that may occur in the event of an earthquake or other significant natural disaster. Additionally, we rely on third-party cloud providers and enterprise applications, technology systems, and our website for our development, marketing, operational support, hosted services, and sales activities. In the event of a catastrophic event, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in our product development, lengthy interruptions in our solutions, and breaches of data security, all of which could have an adverse effect on our results of operations. If we are unable to develop adequate plans to ensure that our business functions continue to operate during and after a disaster and to execute successfully on those plans in the event of a disaster or emergency, our business would be harmed.

Item 2. Unregistered Sales of Equity Securities and Use of Proceeds

(a) Recent Sales of Unregistered Securities.

None.

Item 3. Defaults Upon Senior Securities

None.

Item 4. Mine Safety Disclosures

Not applicable.

Item 5. Other Information

Rule 10b5-1 Trading Arrangements

During the quarter ended April 30, 2026, our directors and officers (as defined in Rule 16a-1(f) under the Exchange Act) adopted or terminated the Rule 10b5-1 trading arrangement (as defined in Item 408(a) of Regulation S-K) described below:

On April 15, 2026, Kiran Choudary, our Chief Financial Officer, adopted a trading arrangement intended to satisfy the affirmative defense conditions of Rule 10b5-1(c). Mr. Choudary's trading arrangement provides for the sale through July 15, 2027 of up to 48,000 shares of our Class A common stock. This represents the maximum number of shares that may be sold pursuant to the 10b5-1 arrangement. The actual number of shares sold will be dependent on the satisfaction of certain conditions set forth in the written plan.

Item 6. Exhibits

Exhibit Number	Description of Exhibit	Incorporated by Reference				
		Form	File No.	Exhibit	Filing Date	Filed Herewith
3.1	Amended and Restated Certificate of Incorporation of Rubrik, Inc.	8-K	001-42028	3.1	4/29/2024	
3.2	Amended and Restated Bylaws of Rubrik, Inc.	8-K	001-42028	3.2	4/29/2024	
31.1	Certification of Principal Executive Officer pursuant to Rules 13a-14(a) and 15d-14(a) under the Securities Exchange Act of 1934, as adopted pursuant to Section 302 of the Sarbanes-Oxley Act of 2002.					X
31.2	Certification of Principal Financial Officer pursuant to Rules 13a-14(a) and 15d-14(a) under the Securities Exchange Act of 1934, as adopted pursuant to Section 302 of the Sarbanes-Oxley Act of 2002.					X
32.1*	Certification of Principal Executive Officer pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002.					X
32.2*	Certification of Principal Financial Officer pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002.					X
101	The following financial information from Rubrik Inc.'s Quarterly Report on Form 10-Q for the quarter ended April 30, 2026 formatted in Inline XBRL (Extensible Business Reporting Language) includes: (i) the Condensed Consolidated Balance Sheets, (ii) the Condensed Consolidated Statements of Operations, (iii) the Condensed Consolidated Statements of Comprehensive Loss, (iv) the Condensed Consolidated Statements of Stockholders' Deficit, (v) the Condensed Consolidated Statements of Cash Flows, and (vi) Notes to the Condensed Consolidated Financial Statements.					X
104	Cover Page Interactive Data File (formatted as inline XBRL and contained in Exhibits 101).					X

* The certifications furnished in Exhibits 32.1 and 32.2 hereto are deemed to accompany this Quarterly Report on Form 10-Q and are not deemed "filed" for purposes of Section 18 of the Exchange Act, or otherwise subject to the liability of that section, nor shall they be deemed incorporated by reference into any filing under the Securities Act or the Exchange Act, irrespective of any general incorporation language contained in such filing.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, as amended, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

Date: June 5, 2026

Rubrik, Inc.	
By:	<u>/s/ Bipul Sinha</u>
Name:	Bipul Sinha
Title:	Chief Executive Officer <i>(Principal Executive Officer)</i>
By:	<u>/s/ Kiran Choudary</u>
Name:	Kiran Choudary
Title:	Chief Financial Officer <i>(Principal Financial and Accounting Officer)</i>

**CERTIFICATION OF PRINCIPAL EXECUTIVE OFFICER PURSUANT TO
RULES 13a-14(a) AND 15d-14(a) UNDER THE SECURITIES EXCHANGE ACT OF 1934,
AS ADOPTED PURSUANT TO SECTION 302 OF THE SARBANES-OXLEY ACT OF 2002**

I, Bipul Sinha, certify that:

1. I have reviewed this Quarterly Report on Form 10-Q of Rubrik, Inc.;
2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;
3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;
4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:
 - a. Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;
 - b. Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;
 - c. Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and
 - d. Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and
5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):
 - a. All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and
 - b. Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: June 5, 2026

By:	/s/ Bipul Sinha
Name:	Bipul Sinha
Title:	Chief Executive Officer (Principal Executive Officer)

**CERTIFICATION OF PRINCIPAL FINANCIAL OFFICER PURSUANT TO
RULES 13a-14(a) AND 15d-14(a) UNDER THE SECURITIES EXCHANGE ACT OF 1934,
AS ADOPTED PURSUANT TO SECTION 302 OF THE SARBANES-OXLEY ACT OF 2002**

I, Kiran Choudary, certify that:

1. I have reviewed this Quarterly Report on Form 10-Q of Rubrik, Inc.;
2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;
3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;
4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:
 - a. Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;
 - b. Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;
 - c. Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and
 - d. Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and
5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):
 - a. All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and
 - b. Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: June 5, 2026

By:	<u>/s/ Kiran Choudary</u>
Name:	Kiran Choudary
Title:	Chief Financial Officer (Principal Financial Officer)

**CERTIFICATION OF PRINCIPAL EXECUTIVE OFFICER PURSUANT TO
18 U.S.C. SECTION 1350, AS ADOPTED PURSUANT TO
SECTION 906 OF THE SARBANES-OXLEY ACT OF 2002**

I, Bipul Sinha, Chief Executive Officer of Rubrik, Inc. (the "Company"), do hereby certify, to the best of my knowledge and pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that:

1. The Quarterly Report on Form 10-Q of the Company for the period ended April 30, 2026 (the "Report"), fully complies with the requirements of Section 13(a) or Section 15(d) of the Securities Exchange Act of 1934, as amended; and
2. The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

Date: June 5, 2026

By:	<u>/s/ Bipul Sinha</u>
Name:	Bipul Sinha
Title:	Chief Executive Officer (Principal Executive Officer)

This certification accompanies the Form 10-Q to which it relates, is not deemed filed with the Securities and Exchange Commission and is not to be incorporated by reference into any filing of the Company under the Securities Act of 1933, as amended, or the Securities Exchange Act of 1934, as amended (whether made before or after the date of the Form 10-Q), irrespective of any general incorporation language contained in such filing.

**CERTIFICATION OF PRINCIPAL FINANCIAL OFFICER PURSUANT TO
18 U.S.C. SECTION 1350, AS ADOPTED PURSUANT TO
SECTION 906 OF THE SARBANES-OXLEY ACT OF 2002**

I, Kiran Choudary, Chief Financial Officer of Rubrik, Inc. (the "Company"), do hereby certify, to the best of my knowledge and pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that:

1. The Quarterly Report on Form 10-Q of the Company for the period ended April 30, 2026 (the "Report"), fully complies with the requirements of Section 13(a) or Section 15(d) of the Securities Exchange Act of 1934, as amended; and
2. The information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

Date: June 5, 2026

By:	<u>/s/ Kiran Choudary</u>
Name:	Kiran Choudary
Title:	Chief Financial Officer (Principal Financial Officer)

This certification accompanies the Form 10-Q to which it relates, is not deemed filed with the Securities and Exchange Commission and is not to be incorporated by reference into any filing of the Company under the Securities Act of 1933, as amended, or the Securities Exchange Act of 1934, as amended (whether made before or after the date of the Form 10-Q), irrespective of any general incorporation language contained in such filing.