Table of Contents

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

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the fiscal year ended January 31, 2025

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	46-4560494
(State or other jurisdiction of incorporation or organization)	(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

Securities registered pursuant to Section 12(g) of the Act: None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☐ No ☒

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark 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 has filed a report on and attestation to its management’s assessment of the effectiveness of its internal control over financial reporting under Section 404(b) of the Sarbanes-Oxley Act (15 U.S.C. 7262(b)) by the registered public accounting firm that prepared or issued its audit report. ☐

If securities are registered pursuant to Section 12(b) of the Act, indicate by check mark whether the financial statements of the registrant included in the filing reflect the correction of an error to previously issued financial statements. ☐

Indicate by check mark whether any of those error corrections are restatements that required a recovery analysis of incentive-based compensation received by any of the registrant's executive officers during the relevant recovery period pursuant to §240.10D-1(b). ☐

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

The aggregate market value of the shares of Class A common stock held by non-affiliates of the Registrant, based on the closing price of the Registrant's shares of Class A common stock on July 31, 2024 as reported by the New York Stock Exchange, was approximately $2.3 billion. In determining the market value of the voting equity held by non-affiliates, shares of common stock of the Registrant beneficially held by each director and officer and each person who owns 10% or more of the Registrant's outstanding common stock have been excluded. This determination of affiliate status is not necessarily a conclusive determination for other purposes.

As of February 28, 2025, Rubrik Inc. had 103,167,994 shares of Class A common stock outstanding, and 86,610,633 shares of Class B common stock outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the Registrant's definitive Proxy Statement related to the 2025 Annual Meeting of Stockholders are incorporated herein by reference in Part III of this Annual Report on Form 10-K to be filed with the Securities and Exchange Commission within 120 days after the end of the fiscal year to which this Annual Report on Form 10-K relates.

Rubrik, Inc.
FORM 10-K
For the Fiscal Year Ended January 31, 2025
TABLE OF CONTENTS

SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

This Annual Report on Form 10-K 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 Annual Report on Form 10-K, 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;
- our ability to compete effectively with existing competitors and new market entrants; and
- our ability to introduce new products on top of our platform.

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

You should not rely on forward-looking statements as predictions of future events. We have based the forward-looking statements contained in this Annual Report on Form 10-K 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 Annual Report on Form 10-K. 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 Annual Report on Form 10-K. 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 Annual Report on Form 10-K. 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 Annual Report on Form 10-K 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 Annual Report on Form 10-K to reflect events or circumstances after the date of this Annual Report on Form 10-K 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 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 offering of Rubrik Security 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 data security 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 data security 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.
- Our use of generative artificial intelligence tools may pose risks to our proprietary software and systems and subject us to legal liability.
- We expect our revenue mix and certain business factors to impact the amount of revenue recognized period to period, which could make period-to-period revenue comparisons not meaningful and make revenue difficult to predict.
- We rely upon third-party cloud providers to host our data security 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

Item 1. Business

We are on a mission to secure the world's data.

Cyberattacks are inevitable. 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. We believe that the future of cybersecurity is data security-if your data is secure, your business is resilient.

We built Rubrik Security Cloud, or RSC, with Zero Trust design principles to secure data across enterprise, cloud, and SaaS applications. 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.

Traditional cybersecurity approaches have failed to not only prevent but also provide recovery from increasingly rampant and sophisticated cyberattacks. At the same time, legacy backup and recovery solutions have significant shortfalls in addressing cyber recovery and data security as they were primarily built for operational and natural disaster recoveries. They were not designed to enable reliable recovery from cyberattacks, nor were they designed to natively deliver cyber threat analytics and event response.

Architecture matters when it comes to securing data. We built a unique software-as-a-service, or SaaS, architecture that combines data and metadata from business applications across enterprise, cloud, and SaaS applications to create self-describing data as a time-series. Self-describing data contains information such as application context, identity, data sensitivity, and application lineage. This allows us to apply artificial intelligence and machine learning directly to business data to understand emergent data threats and deliver cyber recovery. We combined backup and recovery and cybersecurity into a single platform built with a Zero Trust architecture, significantly shrinking the attack surface that exists with legacy solutions. Our Zero Trust Data Security platform assumes that information technology infrastructure will be breached, and nothing can be trusted without authentication. Our data threat engine powered by artificial intelligence and machine learning analyzes the self-describing data time-series to derive security intelligence from data and provide remediation recommendations. Automation is at the core of our architecture ethos. Our automated policy-driven platform delivers data security enforcement, incident response orchestration, and API integrations with the broader security ecosystem.

Our business is indexed to business data growth. Our customers' need for our solutions grows in lockstep with their business data growth and their need for additional data security capabilities. We primarily sell subscriptions to RSC through our sales team and partner network by employing a land and expand sales strategy. We land new customers by selling subscriptions to RSC to secure any one of four distinct types of data: enterprise, unstructured data, cloud, and SaaS applications. Expansion happens along three vectors: the growth of data from applications already secured by Rubrik; new applications secured; and additional data security products. This expansion is driven by a natural flywheel effect in which the value of our platform increases as our customers' data grows across various applications. As organizations manage more data with RSC, they gain deeper insights into their data, strengthen their overall security posture, and reduce compliance risk.

Our Data Security Platform and Products

Rubrik has a unique and purpose-built Zero Trust Data Security approach to help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Despite investment in security tools focused on infrastructure security, encompassing networks, applications, endpoints, and identity, cyberattacks continue unabated. We believe a comprehensive cybersecurity strategy requires data security in addition to traditional infrastructure security approaches. We enable organizations to implement a Zero Trust framework at the data layer, deliver data availability that withstands the aforementioned adverse conditions, and uphold data integrity even when infrastructure is compromised or attacked.

RSC, built with a Zero Trust design, automates data policy management and enforcement, delivers threat analytics and response, and orchestrates rapid recovery. RSC is a cloud native SaaS platform that secures data across disparate sources, allowing customers to have a single point of control from one user interface. RSC is built on a proprietary framework that represents time-series data and metadata generated across enterprise, cloud, and SaaS applications. We build products on top of RSC to address a myriad of use cases that help our customers achieve cyber resilience, from hardening their data security posture to cyber recovery. These use cases include protection and recovery from cyberattacks, malicious insiders, and operational disruptions; orchestration of cyber and operational recovery, failover/failback testing, and cloud migration; sensitive data classification and visibility into over-privileged data access; monitoring for governance, regulatory compliance, and data breaches; and identification, containment, and remediation of ransomware and other security threats.

Our access to time-series data and metadata allows us to deliver a breadth of products that span the following areas:

Data Protection. Cyber-proofs various sources of data in an organization with secure, access-controlled backups. Our data protection products are built for ease of deployment and use, scalability, and rapid recovery from cyberattacks, malicious insiders, and operational disruptions. We offer data protection products to manage enterprise, unstructured data, cloud, and SaaS applications. We also protect identity provider services, such as Microsoft Active Directory and EntraID.

Data Threat Analytics. Detects data threats and identifies the blast radius of a cyberattack to speed up data recovery. Combines Anomaly Detection, Threat Monitoring, and Threat Hunting. Anomaly Detection uses advanced machine learning to detect deletions, modifications, and encryptions. Threat Monitoring continuously monitors for indicators of compromise commonly used by bad actors to establish persistent access, move laterally, or exfiltrate data. Threat Hunting allows incident responders and Security Operations Center (SOC) analysts to hunt for indicators of compromise and determine the initial point, scope, and time of infection.

Data Security Posture. Strengthens cyber posture by locating sensitive data proliferation and identifying data risks. Includes Sensitive Data Monitoring and User Intelligence, which altogether discovers where data lives, sensitivity of data, and user access and activity.

Cyber Recovery. Improves cyber readiness and incident response with orchestrated Cyber Recovery Simulation, Threat Containment, and orchestrated Active Directory Forest Recovery. Cyber Recovery Simulation is used to create, test, and validate recovery plans, while also staying compliant with policy and audit requirements. Cyber Recovery can also be used to recover compromised data within a safe environment for forensic analysis. Threat Containment is used to quarantine data infected with malware so that recovery is enabled without reinfection. Active Directory Forest Recovery orchestrates the recovery of an organization's Active Directory identity service to the desired point in time while avoiding malware reintroduction.

Our products are delivered and consumed via our RSC platform. RSC secures data across enterprise, cloud, and SaaS applications, including:

- **Enterprise:** VMware, Microsoft Hyper-V, Red Hat OpenShift, Microsoft SQL Server, Oracle, PostgreSQL, IBM Db2, Microsoft Windows, Nutanix, Kubernetes, Cassandra, MongoDB, Linux, UNIX, AIX, NAS, Epic, and SAP HANA.
- **Cloud/SaaS:** GCP, Azure, AWS, M365 (Microsoft Teams, SharePoint, Exchange Online, and OneDrive), Salesforce, and Atlassian Jira Cloud.

Architecture Matters

We believe the following attributes of our platform architecture allow us to offer a differentiated approach to data security:

- **Time-Series Data and Metadata.** We design our platform to manage time-series data and metadata as core assets. Our platform combines data and metadata together into self-describing data and records its history over time. To provide a single point of control for data across enterprise, cloud, and SaaS applications, we have constructed a proprietary framework to uniformly represent self-describing data across time. Doing so gives us full context of data and unlocks security use cases, allowing us to build products for cyber recovery and security intelligence.
- **Zero Trust Design.** We employ Zero Trust principles to prevent threats at the data layer. Our use of native immutability, secure protocols, logical air gap, encryption, role-based access controls, multi-factor authentication, and native services uphold data integrity and availability.
- **Data Threat Engine.** We have developed a proprietary machine learning and artificial intelligence based data threat monitoring and management engine to surface anomalous activities and indicators of data breaches. Our self-describing data, which combines data and metadata, gives us the ability to surface emergent data threats, understand data sensitivity, and identify malicious user activities.
- **Automation.** Core to our product design ethos is automation. To consistently secure and manage data at scale, our platform delivers automated end-to-end policy management and enforcement, orchestration of security incident response, and API integrations.

Key Benefits to Our Customers

Leading businesses, governments, and public entities around the world and across all industries and segments choose Rubrik to:

- **Achieve cyber and operational resilience.** Our platform allows organizations to continue business operations even when data and applications are compromised by cyberattacks, malicious insiders, and operational disruptions. From the beginning, we have built our platform with the assumption that security breaches are inevitable and that data availability and integrity must be maintained to minimize business downtime and data loss.

- **Strengthen data security posture.** Our platform helps organizations manage security threats with detection and analysis of security risks. We combine machine learning and threat intelligence to detect data anomalies and unusual behavior, analyze the blast radius of impact, automate ransomware monitoring, and rapidly recover impacted data. Our ability to continuously discover and classify sensitive data, in addition to understanding user access, helps reduce the risk of data exfiltration. Our products can be integrated into security operations' automated playbooks for managing and mitigating ransomware and other data attacks.
- **Secure, govern, and recover data across hybrid multi-cloud and SaaS applications.** We recognize that organizations are in various stages of their cloud and SaaS journeys, and are accumulating data across enterprise, cloud, and SaaS applications. Our platform provides a consistent, policy managed experience across hybrid multi-cloud and SaaS environments, allowing organizations to uniformly deliver data security, governance, and recovery.
- **Comply with data regulations.** Our platform continuously discovers and classifies sensitive data, which provides increasing value to organizations as more data is accumulated across enterprise, cloud, and SaaS applications. This allows organizations to facilitate compliance with evolving data privacy and security regulations, such as GDPR, and reduce risk of double extortion ransomware attacks.
- **Catalog and govern data assets.** We provide a single platform for complete visibility and management as organizations accumulate more data across enterprise, cloud, and SaaS applications. We help organizations understand what data they have, where that data resides, sensitivity of data, and who has unqualified data access. As a result, our customers can shrink their attack surface, reduce risk of security breaches, and accelerate industry regulatory compliance. Our understanding of sensitive data and user access can help enterprises adopt generative AI by setting guardrails to mitigate exposure to compliance, data privacy, and cybersecurity risks.
- **Improve operational efficiency.** As organizations adopt hybrid multi-cloud and SaaS strategies, they encounter many different tools, interfaces, and workflows. Organizations can streamline and standardize data security and management operations with our unified policy automation engine and workflows. This reduces the need for employee training, simplifies security and governance challenges, provides reliable and rapid recoveries, and makes it easier to manage exponential data growth and the accumulation of diverse data sources.

Our Growth Strategy

Key elements of our growth strategy include:

- **Continuing to grow our SaaS solutions.** We believe there is a large and growing market opportunity for our multi-tenant, cloud native solutions as more organizations and customers move their applications and data to the cloud. We plan to continue to invest in the development of RSC, building additional products on top of our platform, and our accompanying go-to-market motion to capitalize on this meaningful opportunity.
- **Growing our customer base.** As cyberattacks increase in scale and sophistication amidst accelerated digitization and ever-evolving data regulations, organizations are rethinking how to secure data across various data sources. We believe we will continue to acquire new customers based on our ability to drive cyber resilience, data security posture management, and regulatory compliance.
- **Expanding within our customer base.** Our existing customer base represents a significant growth opportunity. As our customers accelerate digitization, they adopt more applications and generate more data that must be secured and readily available. We expect to expand our data security products to cover additional scale and scope of data, in addition to cross-selling data governance and compliance products.
- **Innovating and extending our product leadership.** We have a history of creating and introducing disruptive technologies that help our customers achieve business resilience. We intend to continue making significant investments in research and development as well as hiring top technical talent to further increase our product differentiation. In particular, we believe that generative AI will play an important role driving further need for new products to help secure sensitive data and user access. As we continue to invest in our data platform, we will focus on features and functionalities that help enterprises securely adopt generative AI within an evolving threat landscape.
- **Growing and harnessing our partner ecosystem.** We plan to continue investing in building out and leveraging our partner ecosystem to broaden our distribution footprint, drive more platform usage, and drive greater awareness of our platform. Our partner ecosystem includes distributors and resellers, or Channel Partners, system integrators, managed system providers, and technology partners.

- **Expanding our global footprint.** As organizations around the world create more data across enterprise, cloud, and SaaS applications and grapple with an ever-increasing threat level of cyberattacks, including ransomware, and ever-evolving data privacy and security regulations, we believe there is significant opportunity to expand the use of our platform in all major global markets. We have invested in research and development, sales and marketing, and customer support across EMEA and Asia-Pacific regions and expect to continue to do so. We grew our international revenue from such regions from $186.4 million in fiscal year ended 2024 to $250.4 million in fiscal year ended 2025.
- **Pursuing strategic acquisitions.** We have a history of acquiring and integrating strategic products and technologies into our platform to deliver comprehensive data security products to our customers and partners. We intend to continue to pursue strategic teams, technologies, and products to accelerate time-to-market for new data security capabilities and widen the competitive moat for our products and solutions.

Our Customers

We sell to organizations of various sizes that operate across a wide range of industries, including financial services; retail, trade, and transportation; energy and industrials; healthcare and life sciences; public sector and education; technology, media, and communications; and services.

Our Commercial Offerings

RSC is a cloud native SaaS platform that secures data across disparate sources. We build products on top of RSC to address a myriad of use cases that help our customers achieve cyber resilience. Our primary commercial products are as follows:

Data Protection

- **Enterprise Data Protection.** Cyber-proofs enterprise data on physical systems, operating systems, virtual machines, databases, file systems, and containers with air-gapped, immutable, access-controlled backups.
- **Unstructured Data Protection.** Cyber-proofs unstructured file and object data stored on petabyte scale NAS systems with air-gapped, immutable backups.
- **Cloud Data Protection.** Cyber-proofs Azure, AWS, and GCP cloud application data and databases with secure, access-controlled backups.
- **SaaS Data Protection.** Cyber-proofs M365, Salesforce, and Atlassian Jira Cloud data with air-gapped, immutable data resilience and rapid recovery at scale.
- **Identity Provider Services Protection.** Cyber-proofs Microsoft Active Directory and EntraID with immutable backups and rapid recovery across hybrid environments.

Data Threat Analytics

- Detects data threats and identifies the blast radius of a cyberattack to speed up data recovery. Combines Anomaly Detection, Threat Monitoring, and Threat Hunting. Anomaly Detection uses advanced machine learning to detect deletions, modifications, and encryptions. Threat Monitoring continuously monitors for indicators of compromise commonly used by bad actors to establish persistent access, move laterally, or exfiltrate data. Threat Hunting allows incident responders and SOC analysts to hunt for indicators of compromise and determine the initial point, scope, and time of infection.

Data Security Posture

- Strengthens cyber posture by locating sensitive data proliferation and identifying data risks. Includes Sensitive Data Monitoring and User Intelligence, which altogether discovers where data lives, sensitivity of data, and user access and activity. A hardened cyber posture helps customers proactively reduce the risk of cyberattacks, data exfiltration, and sensitive data exposure, in addition to enhancing data governance for generative AI.

Cyber Recovery

- Improves cyber readiness and incident response with orchestrated Cyber Recovery Simulation, Threat Containment, and orchestrated Active Directory Forest Recovery. Cyber Recovery Simulation is used by our customers to create, test, and validate recovery plans, while also staying compliant with policy and audit requirements. Cyber Recovery can also be used to recover compromised data within a safe environment for forensic analysis. Threat Containment quarantines data infected with malware to prevent malware reinfection during recovery. Active Directory Forest Recovery orchestrates the recovery of an organization's Active Directory identity service to the desired point in time while avoiding malware reintroduction.

In addition, we offer Ruby for AI data defense and recovery. Ruby is designed to augment human efforts with its generative AI capabilities, helping customers scale their data security operations with automation, boosting productivity, and bridging the users' skills gap. Ruby uses Microsoft Azure OpenAI Service in combination with our own proprietary, internally developed software. Our proprietary software augments user queries to generate prompts that are submitted to the Azure OpenAI model and also enhances the model output to generate responses presented back to the user. We chose to use Microsoft Azure OpenAI Service based on its security features and because it offers an advanced AI model provisioned in Rubrik's Azure environment such that the data stays within Rubrik's control. For more information regarding the risks related to the use of AI in our business, see the risk factor titled "Our use of generative artificial intelligence tools may pose risks to our proprietary software and systems and subject us to legal liability" in the section titled "Risk Factors."

Our commercial products are used by customers to deliver business resilience against operational failures and cyberattacks. Customers use our Data Protection, Cyber Recovery, and Data Security Posture products to strengthen cyber posture, comply with regulations, and conduct recovery from operational failures, human errors, or natural disasters. During a cyberattack, customers use Data Threat Analytics in addition to the above products to identify, contain, and remediate data threats, determine scope of sensitive data exposure, recover data, and conduct event response.

Our RSC platform is built to be highly flexible and scalable, enabling us to innovate and deliver new data security products in the future.

Our products are available for purchase via four subscription editions to our RSC platform, which are as follows:

- **Foundation Edition.** Keeps data secure and recoverable from cyberattacks and operational failures.
- **Business Edition.** Builds upon Foundation Edition by proactively monitoring for ransomware.
- **Enterprise Edition.** Builds upon Business Edition by continuously monitoring data risk and orchestrating cyber recovery.
- **Enterprise Proactive Edition.** Builds upon Enterprise Edition by adding data security posture management.

Our commercial offerings are accompanied by customer support. We offer several support solutions and capabilities that enhance the value proposition of our software and SaaS solutions:

- **SentryAI.** SentryAI is our proprietary AI deep learning-based platform for system health monitoring, allowing us to deliver proactive customer service throughout the entire customer lifecycle. Our platform uses AI to detect anomalous behavior from telemetry data from our customers. Data analyzed includes performance, security and SLA compliance, and capacity utilization. SentryAI is included within our base support offering.
- **Customer Experience Manager, or CEM.** We offer dedicated customer experience managers to proactively monitor the health of our customers' environments, preemptively detect and resolve emerging issues, including those related to cybersecurity, deliver operational risk management, and recommend strategies for ROI scaling and maximization.
- **Premium-Plus Add-on Support.** Our program provides a CEM and an Assigned Support Engineer, or ASE, for personalized, technical support. Our dedicated teams develop an in-depth understanding of our customers' unique environment requirements, collaborate closely with our customers' operation teams, and provide a direct path to accelerate resolution times.
- **Ransomware Recovery Team.** Our 24x7 Ransomware Recovery Team assists and complements our customers' recovery plans.
- **Education.** We offer Rubrik University, which includes instructor-led training with hands-on labs, on-demand e-learning courses, and certification exams. Education capabilities are targeted at different types of users and delivery modalities to suit end-customer needs. We have instructor-led training and self-paced on-demand courses.
- **Certification Program.** Our certification program enables technical personnel to demonstrate and validate in-depth knowledge of data security by becoming a Rubrik Certified Systems Administrator.

As of February 26, 2025, we achieved an average Net Promoter Score, or NPS, of >80. Our NPS is verified by the Customer Relationship Management Institute LLC.

Our Technology

We have designed a highly differentiated and innovative architecture that is comprised of the following elements:

- **Time-Series Data and Metadata.** Our architecture combines data and metadata from business applications to create self-describing data as a time-series. Self-describing data is important since it contains information such as application context, user identity, data sensitivity, and application lineage, allowing us to understand emergent data threats and deliver cyber recovery. In addition, we have constructed a proprietary framework to uniformly represent this time-series data and metadata from enterprise, cloud, and SaaS applications. Since we have a common way to represent data across a multitude of application sources, we can easily introduce new products on top of our platform.
- **Zero Trust Design.** We employ Zero Trust principles to prevent threats at the data layer. Our usage of native immutability, secure protocols, logical air gap, encryption, role-based access controls, multi-factor authentication, and native services allows us to preserve data integrity and reduce software supply chain risk.
- **Native Immutability.** Our platform was custom designed to provide built-in immutability and preserve data integrity. Our proprietary, append-only file system, combined with data integrity checks, protects data from unauthorized modification, encryption, or deletion, thereby preventing data from being compromised.
- **Secure Protocols.** We architected our platform to allow data access only in an authenticated manner and via secure protocols. Contrast this approach to that of legacy technologies, which offer multi-tier architectures with a full trust security model leveraging insecure network and storage protocols, thereby leaving data vulnerable to corruption, deletion, or theft.
- **Logical Air Gap.** Data is protected by creating a multi-layered barrier between data and malicious actors. Logical processes, such as encryption, hashing, and granular role-based access controls, prevent data from being modified, deleted, or stolen. Our immutable, append-only file system also contributes to establishing a logical air gap by preventing data from being manipulated once written.
- **Native Services.** Our platform provides robust built-in functionality with native services. We do not provide privileged access to third-party applications, thereby reducing the risk of software supply chain attacks.
- **Threat Engine.** Our threat engine uses machine learning and threat intelligence to analyze our time-series data and metadata, detecting anomalies, encryption, content sensitivity, and malware. We can identify the initial point, scope, and time of attack to avoid malware reinfection during recovery.
- **Automation.** Core to our design ethos is automation. To secure data at scale and with consistency, our platform is architected to deliver automated end-to-end policy management, orchestration of security incident response, and API integrations.
- **Policy Automation.** Our fully orchestrated policy engine simplifies how data security objectives are created, enforced, and managed. By providing simplicity and automation in securing data, organizations easily deliver a consistent and uniform data security posture.
- **Integration with Security Operations.** Our solutions integrate with security tools, such as SIEM/SOAR and cloud security, to address a critical gap: security risks and threats at the data layer. Existing security tools pull in data from every corner of the infrastructure (network, applications, endpoints, etc.) but not from the data itself. By integrating continuous monitoring of data and user context, SecOps teams accelerate risk mitigation, incident response, and business resiliency.
- **API-integration.** Our API-first design means that any operation performed via Rubrik's UI is performed through multi-factor authenticated APIs. We offer an extensive collection of pre-built integrations that allow customers to leverage our APIs to integrate data security and data policy management into self-service automation, infrastructure as code, centralized monitoring, log management, and security operations.

Our Go-to-Market Strategy

We primarily sell subscriptions to RSC through our global sales team and partner network. We target the largest organizations worldwide to mid-sized organizations. We sell to smaller customers through a high velocity engagement model driven by our inside sales team.

We utilize a land and expand approach, acquiring new customers and expanding with existing customers. We sell our products through subscriptions to RSC editions and can land in four distinct ways by securing enterprise, unstructured data, cloud, and SaaS applications. After initial purchase, our customers often expand the deployment of our platform within their organization. Expansion happens along three vectors: the growth of data from applications already secured by Rubrik; new applications secured; and additional data security products. This expansion is driven by a natural flywheel effect in which the value of our platform increases as our customers' data grows across various applications. As organizations manage more data with RSC and adopt additional data security products, they gain deeper insights into their data, strengthen their overall security posture, and reduce compliance risk, increasing their overall affinity with Rubrik.

Our sales organization includes sales development, inside sales, sales engineering, and field sales personnel and is segmented both geographically and by the size of prospective customers. We also have dedicated sales teams for the public sector, including federal, state, and local government organizations. Our sales teams identify prospective customers, manage customer accounts, and identify expansion opportunities, while working with our partner network.

We sell our subscriptions to customers through our Channel Partners utilizing a two-tier, indirect fulfillment model. We also offer SaaS products through the marketplaces of our technology alliance partners, including GCP, Azure, and AWS.

Our marketing organization works closely with our sales team to build brand and product awareness and drive sales pipeline. We leverage a mix of outbound marketing tactics such as industry conferences, user events, webinars, and digital programs to target new business, as well as support our upsell and cross-sell efforts. Every year, we organize our user conference, Rubrik Forward, to help our customers realize greater business results through data security. In addition, we leverage inbound marketing activities to generate pipeline and engage in joint marketing activities with our channel and technology alliance partners.

Our Partnerships

Our partnerships consist of Channel Partners, system integrators, managed service providers, and technology partners. Our partner program is designed to maximize technology expertise, technology alliances, and geographic coverage. Our Rubrik Transform Partner Program is a global program that manages our business relationships with our partners.

Our partners help expand the reach of our technology by building brand and product awareness, generating leads, implementing our solutions, providing value-added professional services, and reselling our services. On occasion, we may form deeper strategic relationships, such as our partnership with Microsoft that extends from driving go-to-market activities to co-engineering projects to delivering integrated Zero Trust Data Security products built on Azure.

Research and Development

Our research and development team is responsible for the design, development, testing, operation, and quality of our data security platform. This organization works closely with our cloud operations team to ensure that our platform is available, reliable, and stable. Rubrik Zero Labs is our internal data security research lab that analyzes the global threat landscape, works to eliminate threats with our data security platform, and reports on emerging data security issues. Our research and development leadership team is located in Palo Alto, California, Tel Aviv, Israel and Bangalore, India. We intend to continue to invest in our research and development capabilities to extend our platform and drive innovation of new products to expand our market size and customer impact.

Manufacturing

We rely on a limited number of contract manufacturers, including Super Micro Computer, Inc., or Supermicro, to assemble, test, and load our software onto Supermicro servers to deliver Rubrik-branded commodity servers, or Rubrik-branded Appliances, which the customer enterprise data we secure relies upon. All Rubrik-branded Appliances are currently built on servers designed and supplied by Supermicro. Our Original Equipment Manufacturer Agreement with Supermicro expires in November 2025, with the option to terminate upon each automatic annual renewal thereafter, and does not contain minimum purchase requirements that we must satisfy. We and Supermicro have also agreed to a “Direct-to-Distributor” model, whereby our Channel Partners are authorized to place purchase orders directly with Supermicro, and Supermicro is authorized to sell our Rubrik-branded Appliances directly to our Channel Partners.

Our Competition

The markets we serve are highly competitive and rapidly evolving. Our competition is specific to use cases that we target. We believe we have a unique Zero Trust data architecture. As such, we are not aware of other companies with a Zero Trust Data Security approach that secures and recovers data across enterprise, cloud, and SaaS applications. As customer requirements evolve and new technologies are introduced, we anticipate competition will increase as established or emerging companies develop solutions that address the data security market. Our main competitors fall into the following categories:

- Data management and protection vendors, such as Commvault, Dell EMC, IBM, Veeam, and Cohesity (which recently acquired Veritas’ data protection business);
- Smaller 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, insider threat detection, data classification, incident containment, and other security and data governance technologies.

We believe we compete favorably based on the following competitive factors:

- Ability to converge backup and recovery and cybersecurity in a cloud architecture;

- Ability to automatically manage and secure diverse data types across hybrid cloud, public cloud, and SaaS environments in an easy-to-use, unified platform;
- Ability to provide cyber recovery from a cyberattack;
- Ability to harden data security posture by continuously observing data for security risks;
- Business data access for cyber resilience;
- Ease of deployment, implementation, and use;
- Performance, scalability, and reliability;
- Ease of integration and collection of pre-built integrations with a wide variety of applications, infrastructure, automation, and security products driven by an API-first architecture;
- Time to value and pricing;
- Integrated data governance and compliance capabilities;
- Quality of customer success and professional services; and
- Brand recognition and reputation.

Our Culture and Employees

We consider our culture and employees to be important to our success. Our vision for our people is to establish an environment where our people can grow their careers and feel like they belong and succeed at Rubrik, allowing us to attract, develop, and retain the best talent in the industry to drive Rubrik's success well into the future. We do this through incentivizing and integrating our employees through our competitive rewards and benefits, including equity-based compensation, and by our unique culture.

Our culture is driven by our core company values, and we measure performance against these values:

- **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.

As of January 31, 2025, we had approximately 3,200 full-time employees worldwide. We also engage contractors and consultants. None of our employees are represented by a labor union. In certain countries in which we operate, including Germany and France, we are subject to, and comply with, local labor law requirements, which include works councils and industry-wide collective bargaining agreements. We have not experienced any work stoppages, and we consider our relations with our employees to be good.

Social Responsibility and Community Initiatives

At Rubrik, we are committed to making the world a more secure and better place. In furtherance of our values and this goal, we have joined the Pledge 1% movement, and have committed to donating 1,354,671 shares of our Class A common stock representing approximately 1% of our outstanding capital stock as of immediately prior to our initial public offering over the next 10 years to fund our social impact and environmental, social, and governance initiatives. We plan to commit our time, in addition to our equity and financial resources (including via the donor-advised fund we have established), to support our social responsibility and community initiatives.

Intellectual Property

Intellectual property rights are important to the success of our business. We rely on a combination of patents, copyrights, trademarks, and trade secret laws in the United States and other jurisdictions, as well as license agreements, confidentiality procedures, non-disclosure agreements with third parties, and other contractual protections, to protect our intellectual property rights, including rights in our proprietary technology, software, know-how and brand. We also use open source software in our offering.

As of January 31, 2025, we had 326 issued U.S. patents and patents in various non-U.S. jurisdictions, 237 patent applications pending in the United States, and 5 patent applications pending in various non-U.S. jurisdictions. Our issued patents as of January 31, 2025 expire between April 30, 2034 and August 8, 2043. As of January 31, 2025, we had 12 registered trademarks in the United States, three trademark applications pending in the United States, 19 registered trademarks in various non-U.S. jurisdictions, and four trademark applications pending in various non-U.S. jurisdictions.

Although we rely on intellectual property rights, including contractual protections, to establish and protect our intellectual property, we believe that factors such as the technological and creative skills of our personnel, creation of new services, features and functionality, and frequent enhancements to our platform are essential to establishing and maintaining our technology leadership position.

We control access to and use of our proprietary technology and other confidential information through the use of internal and external controls, including contractual protections with employees, contractors, customers, and partners. We require our employees, consultants, independent contractors, and other third parties to enter into confidentiality and proprietary rights agreements, and we control and monitor access to our software, documentation, proprietary technology, and confidential information. Our policy is to require all employees, consultants, and independent contractors to sign agreements assigning to us any inventions, trade secrets, works of authorship, developments, processes, and other intellectual property generated by them on our behalf and under which they agree to protect our confidential information. In addition, we generally enter into confidentiality agreements with our customers, technology alliance partners, and Channel Partners. See the section titled “Risk Factors” for a more comprehensive description of risks related to our intellectual property.

Available Information

We are headquartered in Palo Alto, California. Our website address is www.rubrik.com. Information found on, or accessible through, our website is not a part of, and is not incorporated into, this Annual Report on Form 10-K. We file electronically with the Securities and Exchange Commission, or the SEC, our annual reports on Form 10-K, quarterly reports on Form 10-Q, current reports on Form 8-K, and amendments to those reports filed or furnished pursuant to Section 13(a) or 15(d) of the Exchange Act. We make available on our website at www.rubrik.com, free of charge, copies of these reports and other information as soon as reasonably practicable after we electronically file such material with, or furnish it to, the SEC. The SEC also maintains an internet site at www.sec.gov that contains reports, proxy and information statements, and other information regarding issuers that file electronically with the SEC.

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 Annual Report on Form 10-K, including the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations" and our 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 $886.5 million, $627.9 million and $599.8 million for the fiscal years ended January 31, 2025, 2024 and 2023, respectively. You should not rely on the revenue growth of any prior quarterly or annual 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, including our transition for new and existing customers to sales of Rubrik Security Cloud ("RSC"), for which an increasing amount of our software revenue will be recognized ratably.

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, and SaaS applications;
- extend our product leadership to expand our addressable market;
- differentiate our data security products from products 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;
- 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. You should not rely on our revenue for any prior quarterly or annual periods as any indication of our future revenue or revenue growth.

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 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 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 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, and SaaS applications, observing the data itself to proactively identify emergent threats, remediating data security threats, and recovering protected data following a cybersecurity event. The market for data security 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 data security 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 offering of RSC, 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. 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. Further, in future periods, we expect our revenue growth to fluctuate, slow, and possibly decline for a number of reasons, including mix shifts in our platform and data security products, as well as the impact on our revenue recognition resulting from our transition from selling our products primarily on the basis of subscription term-based licenses to SaaS subscriptions. The timing for this transition and related implications on our revenue recognition and trends will depend on our ability to transition existing customers to RSC in a timely manner. We are implementing certain initiatives to accelerate our existing customers' migration to RSC as part of our business transition to SaaS, which include enforcement of migration deadlines. These initiatives may be perceived negatively by our customers. For example, these initiatives may require customers to prioritize preparation for their migration over other organizational needs, potentially resulting in diversion of resources. For certain existing customers, the perceived benefits from undertaking the migration may be outweighed by the anticipated time and effort required to prepare for and execute the migration, resulting in potential delays in customers' transition to RSC. We expect these customers may consume our platform and products through a mix of RSC and a transitional license for Cloud Data Management ("RCDM-T"), for an extended period of time, resulting in the continued recognition of a portion of the associated revenue for some of these customers upfront at the time we transfer control of the license to the customer. Conversely, if some or all of these customers complete their transition to RSC sooner than we expect, less revenue would be recognized upfront during this period, which could cause our revenue to be lower than our estimates or forecasts or even result in a decrease in our revenue growth rates. Any of these factors could result in continued fluctuations in our revenue growth and adversely impact our ability to accurately predict our future revenue.

In addition, we operate in a new market for data security 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.

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 data security products. Our sales efforts often involve educating organizations about the uses and benefits of our data security solutions. We may have difficulty convincing organizations of the value of adopting our data security 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 data security 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. 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 data security 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 $(1,154.8) million, $(354.2) million and $(277.7) million for the fiscal years ended January 31, 2025, 2024 and 2023, respectively. As of January 31, 2025 and January 31, 2024, we had an accumulated deficit of $(2,837.3) million and $(1,682.5) million, 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 data security products, 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 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. Moving forward, we expect that substantially all of our new and existing customers will continue to adopt RSC primarily on a SaaS subscription basis. As of the end of fiscal 2024, RSC represented a majority of our total revenue. In addition, we have historically sold Rubrik-branded Appliances to help our customers secure their enterprise data. In the third quarter of fiscal 2023, we began transitioning the sale of Rubrik-branded Appliances from us to our contract manufacturers, and as a result, the amount of revenue we recognize from sales of Rubrik-branded Appliances has and will continue to decline over time. We expect these transitions to adversely affect our revenue as well as our profitability through the fiscal year ending January 31, 2027. However, this timing will depend in part on when a substantial portion of our existing customers complete their transition to RSC.

In addition, following the completion of our IPO, 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 data security 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 products, and increase the volume of their data protected by our data security solutions. 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' spending levels, 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 general economic conditions. Our strategies and initiatives to accelerate the transition of our existing customers to RSC, even if executed properly by our sales and support teams, may result in customer dissatisfaction, the loss of customers, or reduced usage of our platform, any of which would harm our business, financial condition, and results of operations. 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 data security 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 data security 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 data security 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 data security solutions, the failure of our data security solutions to secure, observe, and restore our customers' data, misconfiguration of our data security solutions, the exploitation of any known or unknown vulnerabilities, or the failure of customers to deploy our data security solutions in combination with industry best practices could harm our reputation, result in a loss of, or delay in, market acceptance of our data security 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 data security 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 data security 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 data security 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 data security solutions seek to address. Due to a variety of both internal and external factors, our data security 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 data security 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 data security 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 data security 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. If a high-profile cyberattack occurs with respect to our or another cloud-based security platform or a third-party cloud provider, organizations may lose trust in SaaS platforms and associated products 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 data security solutions and are unable to secure, observe, or restore their data, such customers could discontinue use of our data security solutions, regardless of whether our data security 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 data security 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, in March 2023, we announced that a malicious third party gained unauthorized access to a limited amount of information in one of our non-production information technology testing environments. In addition, in February 2025, we announced that we observed anomalous activity on a server that contained log files, certain of which were accessed by an unauthorized actor. Neither of these incidents resulted in access to data that we secure on behalf of customers or access to our internal code, and there was no 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 data security 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 artificial intelligence ("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.

Any of the previously identified vulnerabilities or cybersecurity threats could cause a security incident or other interruption that could result in 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 may 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) 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 data security solutions, deter new customers from purchasing our data security 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.

Our use of generative artificial intelligence tools may pose risks to our proprietary software and systems and subject us to legal liability.

We use generative AI tools in our business, and we expect to use generative AI tools in the future, including to generate code and other materials incorporated into our products, proprietary software, and systems, and for other internal and external uses. Generative AI refers to deep-learning models that can generate new data, such as text, images, and other content, by analyzing and emulating existing data. 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 to train these generative AI tools. 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. Additionally, our use of third-party generative AI tools to develop source code, text, images, inventions, or other materials may expose us to greater risks than utilizing contracted human developers, as third-party generative AI vendors typically do not provide warranties or indemnities with respect to the output generated by such generative AI tools, and generative AI tools may also hallucinate, providing output that appears correct but is erroneous. Furthermore, some generative 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 a generative AI tool, our AI governance committee (including leaders from our Engineering, Product, Legal, and Information Security teams) performs an analysis and review of the tool, 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 generative 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 generative AI tools, 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 this technology could result in additional compliance costs, regulatory investigations and actions, and lawsuits. For example, we may face 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 proceedings and could require us 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 AI tools to generate code may also present additional security risks because the generated source code may contain security vulnerabilities. Additionally, the vendors of these generative 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 generative 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 generative AI technologies.

We also market some of our own products or features as generative AI tools ("Generative AI Products"). Some of our customers, especially those in highly regulated industries, may be reluctant or unwilling to adopt Generative AI Products. Accordingly, adoption of generative AI features in our products and marketing our products as Generative AI Products could reduce or delay customer adoption. Because generative AI models can hallucinate and provide erroneous output, offering Generative AI Products could result in customer dissatisfaction or potentially claims against us arising out of customer reliance on erroneous output to their detriment. Our Generative AI Products may require us to train or fine-tune AI models using datasets collected by us or from third-party vendors. While we have processes and practices designed to ensure that we and any vendors that we use to source training data have the necessary rights to use such datasets for training our Generative 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 Generative AI Products. For example, we may use publicly available data to train our Generative AI Products that contains 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 Generative AI Products, it may be difficult for us to avoid or identify all instances where a user might nonetheless submit personal data to our Generative AI Products. Furthermore, if we were to receive claims from third parties asserting rights against our use of certain datasets used to train our Generative AI Products, it may be difficult or impossible for us to disentangle our trained models from the subject matter of the claims.

Several jurisdictions around the globe, including in Europe and certain U.S. states, have proposed, enacted, or are considering laws governing AI tools, including the EU's AI Act and the Colorado AI Act. We expect other jurisdictions will adopt similar laws. 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 Generative AI Products and the data we have employed to train them, require us to change our business practices, retrain our Generative 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.

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.

We expect our revenue mix and certain business factors to impact the amount of revenue recognized period to period, which could make period-to-period revenue comparisons not meaningful and difficult to predict.

We expect our revenue mix to vary over time due to a number of factors, including the timing of when customers adopt RSC and the mix of our subscriptions for different data security products. 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. Due to the proportion of our contracts trending from subscription term-based licenses to SaaS subscriptions, the timing of the migration of our existing customers from Cloud Data Management to RSC, as well as the estimates and assumptions used to account for certain customers' Subscription Credits (as defined below) related to their Refresh Rights (as defined below), our revenue may fluctuate and period-to-period revenue comparisons may not be meaningful, and our past results may not be indicative of future performance. We cannot be certain how long these factors may persist. For example, as our existing customers prepare to migrate to RSC, we expect certain of them to consume our solutions through a mix of RSC and RCDM-T during which time we will continue recognizing a portion of the associated revenue upfront. 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 data security 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 data security 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 data security 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, 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 (which recently acquired Veritas' data protection business);
- 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 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 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 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 data security solutions. In the future, further development by these vendors could cause our data security 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 data security 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 data security market is at an early stage and is rapidly evolving. As we are working to create a market for data security from other existing markets that focused on other elements of cybersecurity, our market is at an early stage and rapidly evolving. 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 security and data management sectors 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 platform and data security products. 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 data security 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 data security 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.

There are a limited number of contract manufacturers and original equipment manufacturers of commodity servers that are compatible with our data security solutions, and failure to accurately forecast demand for these commodity servers or successfully manage the relationship with such manufacturers could negatively impact the ability to sell our offerings.

A limited number of Manufacturers produce commodity servers that are compatible with our data security 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. 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, incur increased costs, and our customer relationships may be damaged. 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 suffers delays or disruptions for any reason, including due to recent reports of challenges at Supermicro, experiences increased manufacturing lead-times, capacity constraints, quality control problems in its manufacturing operations, potential delays or increased costs from 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. 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" for additional information regarding our contractual relationship with Supermicro.

Certain of our OEMs carry products that compete with our data security 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 data security 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.

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"), 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 data security 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 data security 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 data security 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 a preferred provider for data security. As such, market adoption of our platform and data security products 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 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 data security 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 existing customers' transition to RSC, including the impact on our revenue recognition and customer retention and expansion;
- 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 data security 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 data security products, including protection of new enterprise, cloud, and SaaS applications, new features, and functionality;
- fluctuations or delays in development, release, or adoption of new features and functionality for our data security 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;
- the number of qualified customers that elect to utilize their Subscription Credits 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 data security 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 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 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 from third parties in order to operate critical functions of our business, including 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 data security 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 data security 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 distributors and resellers, to sell and support our data security solutions. A vast majority of sales of our data security 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 73% and 76% of our revenue for fiscal 2025 and fiscal 2024, 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 data security solutions, or fail to meet the needs of our customers, then our ability to grow our business and sell our data security 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 data security 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 data security 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 data security 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 data security solutions and keep them motivated to sell our data security 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 data security 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. 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 data security 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 may also incur additional compensation and training costs for our sales force, including as part of sales incentive realignment, as we work to migrate existing customers to RSC while ensuring retention and expansion. These additional costs may be higher than we expect depending on timing to complete the transition to RSC and any unforeseen challenges that arise, including due to additional costs faced by customers. Moreover, we could face challenges in our ability to retain sales personnel if the migration to RSC results in the loss of existing customers. 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 data security solutions, particularly with respect to large organizations and government entities. For example, in light of current macroeconomic conditions, we have observed a lengthening of our sales cycles, which may be attributed to higher cost-consciousness around information technology budgets. 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, evolving industry standards, changing regulations, or to changing customer needs, requirements, or preferences, our data security 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 data security solutions, and introduce new data security products and capabilities. The market in which we compete is relatively new and subject to rapid technological change, 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 data security solutions and keep pace with rapid technological change, or if new technologies emerge that are able to deliver competitive products at lower prices, more efficiently, more conveniently, or more securely than our data security solutions, our business, financial condition, and results of operations could be adversely affected.

To remain competitive, we need to continuously modify and enhance our data security 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 solutions to support a variety of use cases. This development effort will require significant engineering, sales, and marketing resources. Any failure to effectively offer data security solutions for these adjacent use cases could reduce customer demand for our platform. Further, our data security 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 data security 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 data security solutions to operate effectively with widely adopted data infrastructure platforms, applications, and technologies would reduce the demand for our data security solutions. If we are unable to respond to customer demand in a cost-effective manner, our data security 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 data security 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 data security solutions with such products and services, our business may be harmed.

The competitive position of our data security 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 data security 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 data security solutions, or our data security 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 data security solutions could result in customer dissatisfaction and harm our business, financial condition, and results of operations.

Our data security 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 data security solutions may be technically complicated, and it may not be easy to maximize the value of our data security solutions without proper implementation, training, and support. Some of our customers have experienced difficulties implementing our data security solutions in the past and may experience implementation difficulties in the future. If we or our customers are unable to implement our data security solutions successfully, customer perceptions of our data security solutions may be impaired, our reputation and brand may suffer, or customers may choose not to renew their subscriptions or purchase additional data security products from us.

Any failure by customers to appropriately implement our data security solutions or any failure of our data security solutions to effectively integrate and operate within our customers' data management infrastructure could result in customer dissatisfaction, impact the perceived reliability of our data security 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 software in our data security solutions, which could negatively affect our ability to sell our data security solutions or subject us to litigation or other actions.

Our data security solutions include third-party open-source software, and we intend to continue to incorporate third-party open-source software in our data security solutions in the future. There is a risk that the use of third-party open-source software 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 software. Although we have internal policies in place designed to monitor the incorporation of open-source software into our data security solutions to avoid such restrictions, we cannot be certain that we have not incorporated open-source software in our data security solutions in a manner that is inconsistent with our licensing model or the licensing terms of any such open-source software. Certain open-source projects also incorporate other open-source software 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 software 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 software licenses could be construed in a manner that imposes unanticipated restrictions or conditions on our use of such software. 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 software, 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 software can lead to greater risks than use of third-party commercial software, as open-source licensors generally do not provide warranties. Use of open-source software 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 software to determine how to compromise our data security solutions.

In addition, licensors of open-source software included in our data security 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 software incompatible with our business, and thus could, among other consequences, prevent us from using or incorporating new updates of such software 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 data security 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 data security 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 data security 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 data security 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 data security solutions may reduce our revenue, cause us to issue credits or pay penalties, cause customers to terminate their subscriptions or data security 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 data security 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 data security 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 data security 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 data security 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 data security solutions.

Components of our data security 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 data security 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 data security solutions. Furthermore, we might be forced to limit the features available in our current or future data security 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 data security solutions. Our data security solutions and the underlying technology may be exported outside of the United States only in compliance with the required export authorizations, including by license, applicability of a license exception, or other appropriate government authorizations, including 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 (including 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 or sanctioned persons, unless otherwise authorized.

While we have taken certain precautions to prevent our data security solutions from being provided in violation of trade controls and are in the process of enhancing our policies and procedures relating to trade controls, our data security solutions may have been in the past, and could in the future be, provided inadvertently and without our knowledge in violation of such laws. Violations of U.S. trade controls 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 and other technology, including import and export licensing requirements, and have enacted laws that could limit our ability to distribute our data security solutions or could limit our customers' ability to implement our data security solutions in those countries. Changes in our data security solutions or future changes in export and import regulations may create delays in the introduction of our data security solutions in international markets, prevent our customers with international operations from deploying our data security solutions globally or, in some cases, prevent the export or import of our data security solutions to certain countries, governments, or persons altogether. From time to time, various governmental agencies have proposed 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 data security solutions by, or in our decreased ability to export or sell our data security solutions to, existing or potential customers with international operations. Any decreased use of our data security solutions or limitation on our ability to export or sell our data security 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 activities. Anti-corruption and anti-bribery laws are interpreted broadly to generally 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 recipients in the public or private sector. As a public company, the FCPA separately requires that we 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 data security solutions and to obtain necessary permits, licenses, and other regulatory approvals. 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 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 require 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 data security 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 parties, 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 data security 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 and funding authorizations, with funding reductions or delays 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 are the subjects of pending litigation, and there remains significant uncertainty about the ways in which agencies will implement the new executive orders. 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. Further, the proceeds we received from the IPO increase the likelihood that we will devote resources to exploring larger and more complex acquisitions and investments than we have previously attempted. 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 data security 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 data security 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 data security 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 data security solutions, succeed in helping customers quickly resolve technical issues or provide effective ongoing support, our ability to sell additional data security 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 data security 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 data security 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 data security 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 data security 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 data security solutions by our personnel could result in claims from our customers for damages related to such misuse. Such misuse of our data security 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 data security 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 data security 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 data security solutions.

Our ability to increase our customer base, achieve broader market adoption and acceptance of our data security 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 data security 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 data security 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 data security solutions and is an important element in attracting new customers. In addition, creating brand awareness of our relatively new data security 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 as a provider of data security solutions 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 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 data security 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 subscriptions to and renewals of our data security solutions, new subscription editions, and new enterprise, cloud, and SaaS applications. As the market for cloud data security evolves, 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 data security solutions, but we may choose not to introduce or be unsuccessful in implementing future price increases. Furthermore, since we have limited experience pricing RSC editions and solutions, 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 data security 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 financings, sales of our data security solutions, and the utilization of debt products, including our Amended Credit Facility (as described in the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations—Liquidity and Capital Resources"). 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 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. If we incur additional debt, the debt holders would have rights senior to holders of common stock to make claims on our assets, and the terms of any debt could restrict our operations, including our ability to pay dividends on our Class A common stock. Furthermore, if we issue additional equity securities, stockholders will experience dilution, and the new equity securities could 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.

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

Our data security 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 data security solutions to our customers outside of the United States, 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 rising interest rates, bank failures, international trade relations, including tariffs and trade tensions, political turmoil, including the conflict in the Middle East and the ongoing conflict between Russia and Ukraine, potential 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. As an example, in the United States, capital markets have experienced and continue to experience volatility and disruption. Furthermore, inflation rates in the United States have recently increased to levels not seen in decades. 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 surrounding area, and our growth, business, and results of operations could be further negatively impacted if the current conflict in Israel and the surrounding area continues, worsens, or expands to other nations or regions. 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 data security 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 data security 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 data security 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 data security solutions are complex, we are also often required to invest significant time and other resources to train and familiarize potential customers with our data security 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 data security 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 data security 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 data security 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 data security 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 data security 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; and
- other practical, resource, or business limitations on our ability to detect and prevent infringement or misappropriation of our rights and to enforce our rights.

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 31% and 32% of our total revenue for fiscal 2025 and fiscal 2024, 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, 2025, 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 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 is 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.

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 data security 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 data security 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 control 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 for the fiscal year ending January 31, 2026. This assessment will need 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 will be required to attest to the effectiveness of our internal control over financial reporting in our first annual report required to be filed with the SEC following the date we are no longer an "emerging growth company." We have recently commenced the costly and challenging process of compiling the system and processing documentation necessary to perform the evaluation needed to comply with Section 404 of the Sarbanes-Oxley Act ("Section 404"), but we may not be able to complete our evaluation, testing, and any required remediation in a timely fashion once initiated. Our compliance with Section 404 will require that we incur substantial expenses and expend significant management efforts. Although we currently have an internal audit group, we will need to hire additional accounting and financial staff with appropriate public company experience and compile the system and process documentation necessary to perform the evaluation needed to comply with Section 404.

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 data security solutions without infringing, misappropriating, or otherwise violating the intellectual property rights of third parties. However, we may not be aware that our data security 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 data security 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 data security 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 may still in the future become subject to claims alleging such violations. Litigation may be necessary to defend against 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, combined with our transition from a privately held to a publicly traded company, 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 data security solutions by international organizations;
- changes in a specific country's or region's political or economic conditions;
- the need to adapt and localize our data security 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 the surrounding area 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. For example, 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. Effective January 1, 2022, the Tax Act eliminated the option to deduct research and development expenses for tax purposes in the year incurred and instead requires taxpayers to capitalize and subsequently amortize such expenses over five years for research activities conducted in the United States and over 15 years for research activities conducted outside the United States. Although there have been legislative proposals to repeal or defer the capitalization requirement to later years, there can be no assurance that the provision will be repealed or otherwise modified. 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. 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 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 the reallocation of taxing rights in respect of certain profits of multinational enterprises above a fixed profit margin to the jurisdictions within which they carry on business (subject to certain revenue threshold rules, which we do not currently meet but may meet in the future), referred to as “Pillar One,” and imposing 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. Based on our current understanding of the minimum revenue thresholds contained in the Pillar Two proposal, we currently expect to fall within the scope of its rules in the short term. The OECD has issued administrative guidance providing transition and safe harbor rules in relation to the implementation of the Pillar Two proposal. We are monitoring developments and evaluating the potential impacts of these new rules, including on our effective tax rates, and considering our eligibility to qualify for these safe harbor rules. 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 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 are considering or 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 have adopted or may 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, 2025, we had net operating loss ("NOL"), carryforwards for federal and state income tax purposes of $1,346.1 million and $626.2 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 2028 for state purposes if not utilized. Under current law, U.S. federal NOLs incurred in taxable years beginning after December 31, 2017 may be carried forward indefinitely, but such federal NOLs 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 NOLs 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 NOLs to offset future taxable income. We have experienced ownership changes 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 NOLs 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 consolidated financial statements and accompanying notes appearing elsewhere in this Annual Report on Form 10-K. 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 our Refresh Rights and 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 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. The term loans mature in August 2028, and the interest payments associated with the term loans are due quarterly. The Amended Credit Facility refinanced and replaced the term loan facility we previously entered into in June 2022 with Goldman Sachs BDC, Inc., as administrative agent, and the other lenders party thereto.

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.

A substantial majority of our existing indebtedness consists of indebtedness under our Amended Credit Facility with Goldman Sachs BDC, Inc., as administrative agent, and the other lenders party thereto, which matures in August 2028. We may not be able to further refinance the existing indebtedness because of the amount of our debt, debt incurrence restrictions under our debt agreements, 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. Although the financing documents that govern substantially all of our indebtedness contain restrictions on the incurrence of additional indebtedness and entering into certain types of other transactions, these restrictions are subject to a number of qualifications and exceptions. Additional indebtedness incurred in compliance with these restrictions could be substantial. To the extent we incur additional indebtedness, the significant leverage risks described above would be exacerbated.

The terms of the financing documents governing our term loan and credit facilities restrict our current and future operations, particularly our ability to respond to changes or to take certain actions.

The financing documents governing our credit facilities impose significant operating and financial restrictions on us and may limit our ability to engage in acts that may be in our long-term best interests, including restrictions on our ability to:

- incur or guarantee additional indebtedness;
- pay dividends and make other distributions on, or redeem or repurchase, capital stock;
- make certain investments;
- incur certain liens;
- enter into transactions with affiliates;
- merge or consolidate;
- enter into agreements that restrict the ability of subsidiaries to make certain intercompany dividends, distributions, payments, or transfers; and
- transfer or sell assets, including our intellectual property.

As a result of the restrictions described above, we will be limited as to how we conduct our business, and we may be unable to raise additional debt or equity financing to compete effectively or to take advantage of new business opportunities. The terms of any future indebtedness we may incur could include more restrictive covenants. We cannot assure you that we will be able to maintain compliance with these covenants in the future and, if we fail to do so, that we will be able to obtain waivers from the lenders or amend the covenants.

Our failure to comply with the restrictive covenants described above as well as other terms of our indebtedness or the terms of any future indebtedness we may incur from time to time could result in an event of default, which, if not cured or waived, could result in our being required to repay these borrowings before their due date. If we are forced to refinance these borrowings on less favorable terms or are unable to refinance these borrowings, our business, financial condition, and results of operations could be adversely affected.

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 January 31, 2025, holders of our Class B common stock, including our executive officers and directors and their affiliates, together hold approximately 95% of the voting power of our outstanding capital stock, and our directors, executive officers, and principal stockholders beneficially own approximately 45% of our outstanding classes of common stock as a whole, but control approximately 90% 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 data security solutions;
- changes in our projected operating and financial results;
- changes in laws or regulations applicable to our data security solutions;
- announcements by us or our competitors of significant business developments, acquisitions, or new data security 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;
- 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 January 31, 2025, there were 9,570,134 shares of Class B common stock issuable upon the exercise of options and 18,039,511 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.

Our issuance of additional capital stock in connection with financings, acquisitions, investments, our equity incentive plans, or otherwise 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. 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. In addition, our Amended Credit Facility contains restrictions on our ability to pay cash dividends on our Class A Common Stock. 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 are an "emerging growth company," and we cannot be certain if the reduced reporting and disclosure requirements applicable to emerging growth companies will make our Class A common stock less attractive to investors.

We are an "emerging growth company," as defined in the JOBS Act, and we may take advantage of certain exemptions from various reporting requirements that are applicable to other public companies that are not "emerging growth companies," including the auditor attestation requirements of Section 404, reduced disclosure obligations regarding executive compensation in our periodic reports and proxy statements, and exemptions from the requirements of holding a nonbinding advisory vote on executive compensation and stockholder approval of any golden parachute payments not previously approved. Pursuant to Section 107 of the JOBS Act, as an emerging growth company, we have elected to use the extended transition period for complying with new or revised accounting standards until those standards would otherwise apply to private companies. As a result, our consolidated financial statements may not be comparable to the financial statements of issuers who are required to comply with the effective dates for new or revised accounting standards that are applicable to public companies, which may make our Class A common stock less attractive to investors. In addition, if we cease to be an emerging growth company, we will no longer be able to use the extended transition period for complying with new or revised accounting standards.

We will remain an emerging growth company until the first to occur of: (1) the last day of the year following the fifth anniversary of our IPO; (2) the last day of the first year in which our annual gross revenue is $1.235 billion or more; (3) the date on which we have, during the previous rolling three-year period, issued more than $1.0 billion in non-convertible debt securities; and (4) the date we qualify as a "large accelerated filer," with at least $700 million of equity securities held by non-affiliates.

We cannot predict if investors will find our Class A common stock less attractive if we choose to rely on these exemptions. For example, if we do not adopt a new or revised accounting standard, our future results of operations may not be as comparable to the results of operations of certain other companies in our industry that adopted such standards. If some investors find our Class A common stock less attractive as a result, there may be a less active trading market for our Class A common stock, and our stock price may be more volatile.

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, which we expect to further increase after we are no longer an "emerging growth company." 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 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.

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 Securities Exchange Act of 1934, as amended (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 data security 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 1B. Unresolved Staff Comments

None.

Item 1C. Cybersecurity

Risk management and strategy

We have implemented and maintain various information security processes designed to identify, assess and manage material risks from cybersecurity threats to our critical computer networks, third party hosted services, communications systems, hardware and software, and our critical data, including intellectual property, confidential information that is proprietary, strategic or competitive in nature, and sensitive data and applications of our customers ("Information Systems and Data").

Our Chief Information Security Officer (“CISO”) and the direct reports to the CISO (including the Senior Director of Information Security and the Senior Director for Governance, Risk and Compliance, collectively, the “CISO Team”) help identify, assess and manage the Company’s cybersecurity threats and risks, including through the use of a risk register. The CISO Team identifies and assesses risks from cybersecurity threats by monitoring and evaluating our threat environment using various methods including, for example, manual and automated tools, subscribing to reports and services that identify cybersecurity threats, analyzing reports of threats and actors, conducting scans of the threat environment, evaluating our and our industry’s risk profile, evaluating threats reported to us, internal and/or external audits, conducting vulnerability assessments to identify vulnerabilities, use of external intelligence feeds, and third-party-conducted red/blue team testing and tabletop incident response exercises.

Depending on the environment, we implement and maintain various technical, physical, and organizational measures, processes, standards and policies designed to manage and mitigate material risks from cybersecurity threats to our Information Systems and Data, including, for example: an incident response plan and/or incident response policy, incident detection and response, a vulnerability management policy, disaster recovery/business continuity plans, risk assessments, implementation of security standards/certifications, encryption of data, network security controls, access controls, physical security, vendor risk management program, employee training, penetration testing, cybersecurity insurance, dedicated cybersecurity staff/officer, and systems monitoring.

Our assessment and management of material risks from cybersecurity threats are integrated into the Company’s overall risk management processes. For example, (1) cybersecurity risk is identified in and a component of the Company’s risk register; (2) the CISO Team works with management to prioritize our risk management processes and mitigate cybersecurity threats that are more likely to lead to a material impact to our business; and (3) our information security team evaluates material risks from cybersecurity threats against our overall business objectives and reports to the board of directors, which evaluates our overall enterprise risk.

We use third-party service providers to assist us from time to time to identify, assess, and manage material risks from cybersecurity threats, including for example professional services firms (including legal counsel), threat intelligence service providers, cybersecurity consultants, cybersecurity software providers, penetration testing firms, dark web monitoring services, and forensic investigators.

We also use third-party service providers to perform a variety of functions throughout our business, such as application providers, hosting companies, and supply chain resources. We have a vendor management program to manage cybersecurity risks associated with our use of these providers. The program includes risk assessment for each vendor, security questionnaires, review of the vendor's written security program, review of security assessments and reports, audits, calls with vendors security personnel, and contractual obligations regarding cybersecurity imposed on each vendor. Depending on the nature of the services provided, the sensitivity of the Information Systems and Data at issue, and the identity of the provider, our vendor management process may involve different levels of assessment designed to help identify cybersecurity risks associated with a provider and impose contractual obligations related to cybersecurity on the provider.

For a description of the risks from cybersecurity threats that may materially affect the Company and how they may do so, see our risk factors under Part I. Item 1A. Risk Factors in this Annual Report on Form 10-K.

Governance

Our board of directors addresses the Company’s cybersecurity risk management as part of its general oversight function. The board of directors is responsible for overseeing Company’s cybersecurity risk management processes, including oversight and mitigation of risks from cybersecurity threats.

Our cybersecurity risk assessment and management processes are implemented and maintained by certain Company management, including the CISO Team, along with other members of management.

Our CISO Team is responsible for hiring appropriate personnel, helping to integrate cybersecurity risk considerations into the Company’s overall risk management strategy, and communicating key priorities to relevant personnel. The CISO Team is also responsible for approving budgets, helping prepare for cybersecurity incidents, approving cybersecurity processes, and reviewing security assessments and other security-related reports.

Our cybersecurity incident response processes are designed to escalate certain cybersecurity incidents to members of management depending on the circumstances, including our crisis management team. The CISO Team works with our crisis management team to help the Company mitigate and remediate cybersecurity incidents of which they are notified. In addition, the Company’s incident response processes include reporting to the board of directors for certain cybersecurity incidents.

The board of directors receives periodic reports from the CISO team concerning the Company’s significant cybersecurity threats and risk and the processes the Company has implemented to address them. The board of directors also receives various reports, summaries or presentations related to cybersecurity threats, risk and mitigation.

Item 2. Properties

We are headquartered in Palo Alto, California, where we lease approximately 81,031 square feet pursuant to a lease which expires in 2027. We currently lease other office space throughout the United States and globally, including in, Austin, Texas; Morrisville, North Carolina; Lawrence, Kansas; Reston, Virginia; Bangalore, India; Cork, Ireland; Amsterdam, Netherlands; Tel Aviv, Israel; and Sydney, Australia. We do not own any real property. We believe that our facilities are adequate to meet our current needs.

Item 3. 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 4. Mine Safety Disclosures

Not applicable.

PART II

Item 5. Market for Registrant's Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities

Market Information of our Class A Common Stock

Our Class A common stock, par value $0.000025 per share, is listed on the New York Stock Exchange, under the symbol "RBRK" and began trading on April 25, 2024. Prior to that date, there was no public trading market for our Class A common stock.

Holders of Common Stock

As of February 28, 2025, there were 27 stockholders of record of our Class A common stock and 52 stockholders of record of our Class B common stock. The actual number of holders of our Class A common stock is greater than the number of record holders and includes stockholders who are beneficial owners, but whose shares are held in street name by brokers or other nominees. The number of holders of record presented here also does not include stockholders whose shares may be held in trust by other entities.

Dividend Policy

We have never declared or paid cash dividends on our capital stock. We currently intend to retain all available funds and future earnings, if any, to fund the development and expansion of our business, and we do not anticipate paying any cash dividends in the foreseeable future. Any future determination regarding the declaration and payment of dividends, if any, will be at the discretion of our board of directors and will depend on then-existing conditions, including our financial condition, results of operations, contractual restrictions, capital requirements, business prospects, and other factors our board of directors may deem relevant. Our Amended Credit Facility contains restrictions on our ability to pay cash dividends on our capital stock. Additionally, our ability to pay dividends may be further restricted by agreements we may enter into in the future.

Recent Sales of Unregistered Securities

None.

Use of Proceeds

On April 29, 2024, we completed our IPO, in which we issued and sold 23,500,000 shares of our Class A common stock, at a public offering price of $32.00 per share (the "IPO Price"). We received net proceeds of approximately $710.3 million, after deducting underwriting discounts and commissions of $41.7 million. In May 2024, our underwriters exercised their option to purchase an additional 3,472,252 shares of our Class A common stock at the IPO Price of $32.00 per share. We received net proceeds of approximately $104.9 million, net of underwriters' discounts and commissions. All shares sold were registered pursuant to a registration statement on Form S-1 (File No. 333-278434), as amended (the "Registration Statement"), declared effective by the SEC on April 24, 2024. Goldman Sachs & Co. LLC acted as the representative of the underwriters for the offering. The offering terminated after the sale of all securities registered pursuant to the Registration Statement. No payments for such expenses were made directly or indirectly to (i) any of our officers or directors or their associates, (ii) any persons owning 10% or more of any class of our equity securities, or (iii) any of our affiliates.

There has been no material change in the planned use of proceeds from our IPO as described in our Final Prospectus for the IPO dated as of April 24, 2024 and filed with the SEC pursuant to Rule 424(b)(4) on April 26, 2024.

Issuer Purchases of Equity Securities

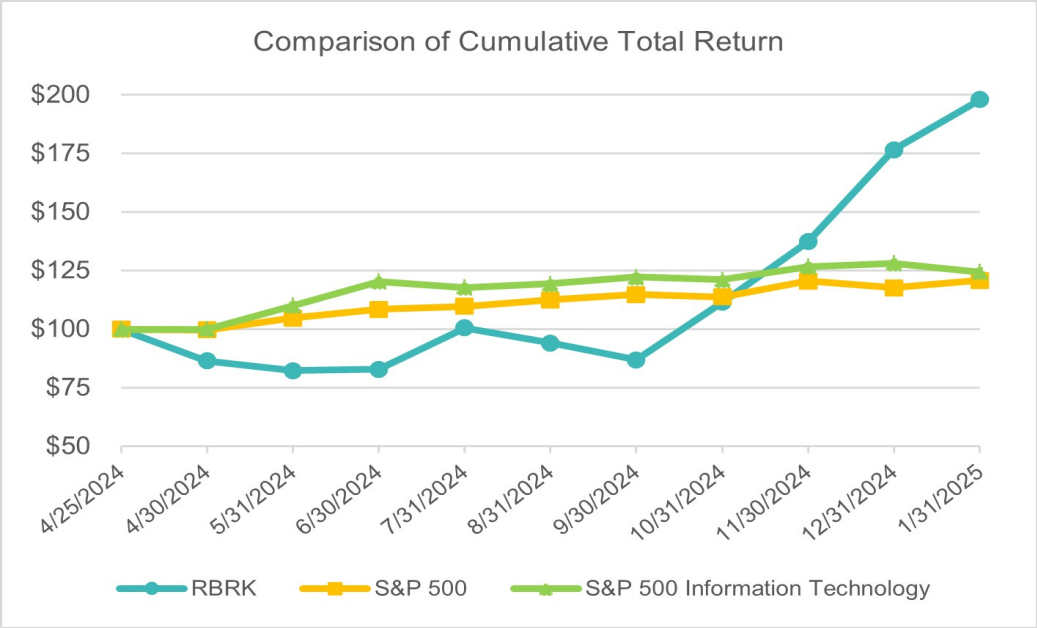
None.

Stock Performance Graph

This performance graph shall not be deemed "soliciting material" or to be "filed" with the SEC for purposes of Section 18 of the Exchange Act, or otherwise subject to the liabilities under that Section, and shall not be deemed to be incorporated by reference into any of our filings under the Securities Act.

Table of Contents

The graph below shows the cumulative total return to our stockholders between April 25, 2024 (the date that our Class A common stock commenced trading on the New York Stock Exchange) through January 31, 2025 in comparison to the S&P 500 Index and the S&P 500 Information Technology Index. The graph assumes (i) that $100 was invested in each of our Class A common stock, the S&P 500 Index, and the S&P 500 Information Technology Index at their respective closing prices on April 25, 2024 and (ii) reinvestment of gross dividends. The stock price performance shown in the graph represents past performance and should not be considered an indication of future stock price performance.



Item 6. [Reserved]

Item 7. 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 consolidated financial statements and related notes appearing elsewhere in this Annual Report on Form 10-K. Some of the information contained in this discussion and analysis, including information with respect to our planned investments in our research and development, sales and marketing, and general and administrative functions, includes forward-looking statements that involve risks and uncertainties as described under the heading "Special Note About Forward-Looking Statements" in this Annual Report on Form 10-K. You should review the disclosure under the heading "Risk Factors" in this Annual Report on Form 10-K 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 Annual Report on Form 10-K 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.

A discussion regarding our financial condition and results of operations for the fiscal year ended January 31, 2024 compared to the fiscal year ended January 31, 2025 is presented below. A discussion regarding our financial condition and results of operations for the fiscal year ended January 31, 2023 compared to the fiscal year ended January 31, 2024 can be found in "Management's Discussion and Analysis of Financial Condition and Results of Operations" in the final prospectus for our initial public offering ("IPO") dated as of April 24, 2024 and filed with the Securities and Exchange Commission ("SEC") pursuant to Rule 424(b)(4) on April 26, 2024.

Overview

We are on a mission to secure the world's data.

Cyberattacks are inevitable. 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. We believe that the future of cybersecurity is data security—if your data is secure, your business is resilient.

We built Rubrik Security Cloud ("RSC") with Zero Trust design principles to secure data across enterprise, cloud, and SaaS applications. 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 product. In addition, we began offering new SaaS subscription products, Anomaly Detection and Sensitive Data Monitoring. In fiscal 2020, we continued our business evolution to a subscription pricing model by offering our CDM platform 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 comprehensive Zero Trust Data Security platform. RSC culminates our early vision of providing one point of control to secure data across enterprise, cloud, and SaaS applications. 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 offer Subscription Credits to qualifying customers. 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. As of the end of fiscal 2024, RSC represented a majority of our total revenue.

We recognize revenue from the sales of our RSC platform (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.

We expect new and existing customers to continue to adopt RSC. Our new customers have generally been rapidly adopting the RSC platform. We are actively migrating our existing customers from our legacy CDM capabilities to RSC. As part of this migration, we expect certain existing customers to consume our platform and products through a mix of RSC and a transitional CDM license ("RCDM-T"), during which time we expect to continue recognizing a portion of the associated revenue from these customers upfront at the time we transfer control of the license to the customer. We cannot predict how long these customers will use this mix before they complete their transition. In addition, our revenue will fluctuate when qualified customers choose to exercise or forfeit their Subscription Credits (which are customer options that are accounted for as material rights) upon their associated expiration date.

Key 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, and SaaS applications. 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 protect enterprise, unstructured data, cloud, and SaaS applications, securing large amounts of their data. 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.

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 subscription contracts as of the measurement date, assuming any contract that expires during the next 12 months is renewed on existing terms. Subscription contracts include offerings for our RSC platform and related data security SaaS solutions, term-based licenses for our RSC-Private platform 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 products like Anomaly Detection and Sensitive Data Monitoring. 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:

	January 31,	
	2025	2024
	(in thousands, except percentages)	
Subscription ARR	$ 1,092,584	$ 784,029
% growth	39 %	47 %

Subscription ARR does not include any maintenance revenue associated with perpetual licenses, which we generally no longer offer. Of the 39% and 47% growth, approximately 2 percentage points and 4 percentage points of growth for the twelve months ended
January 31, 2025 and 2024, respectively, were a result of transitioning our existing maintenance customers to our subscription editions. We expect the contributions to growth from these transitions to subside in fiscal 2026.

Cloud Annual Recurring Revenue, or Cloud ARR

Cloud ARR is calculated as the annualized value of our active cloud-based subscription contracts 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 subscription contracts include RSC and RSC-Government (excluding RSC-Private). Cloud ARR also includes SaaS subscription products 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:

	January 31,	
	2025	2024
	(in thousands, except percentages)	
Cloud ARR	$ 875,602	$ 524,767
% growth	67 %	119 %

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:

	January 31,	
	2025	2024
Average subscription dollar-based net retention rate	over 120 %	over 130 %

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:

	January 31,	
	2025	2024
Customers with $100,000 or more in Subscription ARR	2,246	1,742
% growth	29 %	45 %

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, including discretionary cash payments of our debt interest expense pursuant to the terms of our Amended Credit Facility and prepayments of other spend. Additionally, free cash flow is not a substitute for cash 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 $21.6 million, $(24.5) million and $(15.0) million for the fiscal year ended January 31, 2025, 2024 and 2023, respectively. Free cash flow for the fiscal year ended January 31, 2025 includes a cash outlay of $22.8 million for employer payroll taxes due to the vesting of certain equity awards in conjunction with the initial public offering. The improvement in free cash flow was primarily due to higher sales that were offset by higher expenses including expenses from Laminar operations, which was acquired in August 2023, a decrease in contract term due to the growth of our Cloud and SaaS products, and an increasing mix of annual and consumption payments from customers. 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 and our multi-year cash collection 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 used in operating activities for the periods presented:

	Year Ended January 31,		
	2025	2024	2023
		(in thousands)	
Net cash provided by (used in) operating activities	$ 48,228	$ (4,518)	$ 19,287
Less: Purchases of property and equipment	(16,885)	(12,333)	(25,017)
Less: Capitalized internal-use software	(9,714)	(7,675)	(9,281)
Free cash flow	$ 21,629	$ (24,526)	$ (15,011)
Net cash used in investing activities	$ (383,442)	$ (93,623)	$ (125,188)
Net cash provided by financing activities	$ 398,023	$ 95,949	$ 171,823

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 2%, (12)%, and (38)% for the 12 months ended January 31, 2025, 2024 and 2023, respectively. For the 12 months ended January 31, 2025, the non-GAAP expenses includes the recognition of $22.8 million for employer payroll taxes due to the vesting of certain equity awards in conjunction with the initial public offering. The increase in Subscription ARR Contribution Margin was primarily driven by the strong year-over-year growth in Subscription ARR, compared to 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.

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 cost of revenue and (ii) non-GAAP operating expenses to operating expenses.

	Twelve Months Ended January 31,		
	2025	2024	2023
	(in thousands, except percentages)		
Subscription cost of revenue	$ 215,036	$ 97,927	$ 62,294
Stock-based compensation expense	(49,514)	(45)	(53)
Stock-based compensation from amortization of capitalized internal-use software	(273)	(153)	(287)
Amortization of acquired intangibles	(3,673)	(1,676)	(822)
Non-GAAP subscription cost of revenue	$ 161,576	$ 96,053	$ 61,132
Operating expenses	$ 1,754,828	$ 789,436	$ 679,353
Stock-based compensation expense	(846,872)	(5,652)	(6,727)
Non-GAAP operating expenses	$ 907,956	$ 783,784	$ 672,626
Subscription ARR	$ 1,092,584	$ 784,029	$ 532,929
Non-GAAP subscription cost of revenue	(161,576)	(96,053)	(61,132)
Non-GAAP operating expenses	(907,956)	(783,784)	(672,626)
Subscription ARR Contribution	$ 23,052	$ (95,808)	$ (200,829)
Subscription ARR Contribution Margin	2 %	(12)%	(38)%

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.

Our revenue will fluctuate based on the timing for transitioning our existing customers to RSC, including the RCDM-T licenses offered to existing customers, sales of RSC-Private, and when qualified customers choose to exercise or forfeit their Subscription Credits, the customer options that are accounted for as material rights. These expected trends, when combined with the transition of the sale of Rubrik-branded Appliances from us to our contract manufacturers, will limit and cause fluctuations to our revenue growth through fiscal 2027. We primarily measure our business on the basis of Subscription ARR, as we believe it best reflects our actual growth and our growth prospects.

Subscription Revenue

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

SaaS includes SaaS subscription products 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 platform 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, 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 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 subscription capabilities are primarily sold as editions which bundle multiple products and include the Foundation Edition, Business Edition, Enterprise Edition, and Enterprise Proactive 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.

As customers continue to adopt or transition to RSC, we expect the ratable portion of our subscription revenue to increase. We expect certain customers to consume our platform and products through a mix of RSC and RCDM-T as they complete the migration, which will result in a recognition of a portion of the associated revenue for these customers upfront. Furthermore, our subscription revenue will also fluctuate when qualified customers choose to exercise or forfeit their customer options that are accounted for as material rights. In fiscal 2025, subscription revenue saw some modest benefits as customers exercise or forfeit their Subscription Credits. We expect to see some further benefits through fiscal 2027 that we do not expect to continue in the long-term. The combination of both of these factors will limit and cause fluctuations in our subscription revenue growth through fiscal 2027, depending in part on the timing of our existing customers' transition to RSC.

Maintenance Revenue

Maintenance revenue represents fees earned from software updates on a when-and-if-available basis, telephone support, integrated web-based support, and Rubrik-branded Appliance maintenance relating to our perpetual licenses. Maintenance revenue is recognized ratably over the term of the service period. We expect our maintenance revenue to decrease as we drive adoption of RSC for existing maintenance customers and the transition to be largely completed by the end of fiscal 2026.

Other Revenue

Other revenue represents fees earned from sales of Rubrik-branded Appliances and professional services. 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. In the third quarter of fiscal 2023, we began transitioning the sale of Rubrik-branded Appliances from us to our contract manufacturers and this was largely completed in fiscal 2025. 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 Maintenance Revenue

Cost of maintenance revenue primarily includes employee compensation and related expenses associated with customer support from our perpetual licenses. Over the long-term, we expect our cost of maintenance revenue to decrease as our maintenance revenue decreases.

Cost of Other Revenue

Cost of other revenue primarily includes the cost of Rubrik-branded Appliances and professional services. We expect cost of other revenue as a percentage of total cost of revenue to decrease due to the sales of Rubrik-branded Appliances transitioning from us to our contract manufacturers which 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

With increased adoption of RSC, we expect SaaS revenue to increase as a percentage of total revenue, which we expect will result in an increase in associated hosting costs. As customers adopt RSC, 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 platform.

Maintenance Gross Margin

We expect maintenance revenue to decrease as a percentage of total revenue, which we expect will result in a decrease in maintenance costs. We expect our maintenance margin to fluctuate until the end of fiscal 2026 as maintenance revenue and related costs decline as customers adopt RSC.

Other Gross Margin

We expect sales of Rubrik-branded Appliances to decrease as we transition the sale from us to contract manufacturers, which will result in a decrease in associated Rubrik-branded Appliance costs. The transition of the sale of Rubrik-branded Appliances 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, 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 federal and 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 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.

	Year Ended January 31,		
	2025	2024	2023
	(in thousands)		
Revenue			
Subscription	$ 828,740	$ 537,869	$ 385,272
Maintenance	18,408	38,745	76,220
Other	39,396	51,278	138,327
Total revenue	886,544	627,892	599,819
Cost of revenue			
Subscription[(1)]	215,036	97,927	62,294
Maintenance[(1)]	6,068	6,472	15,059
Other[(1)]	44,644	40,563	104,661
Total cost of revenue	265,748	144,962	182,014
Gross profit	620,796	482,930	417,805
Operating expenses			
Research and development[(1)]	531,615	206,527	175,057
Sales and marketing[(1)]	867,518	482,532	417,542
General and administrative[(1)]	355,695	100,377	86,754
Total operating expenses	1,754,828	789,436	679,353
Loss from operations	(1,134,032)	(306,506)	(261,548)
Interest income	25,353	11,216	5,140
Interest expense	(41,253)	(30,295)	(11,709)
Other income (expense), net	1,480	(1,884)	(1,033)
Loss before income taxes	(1,148,452)	(327,469)	(269,150)
Income tax expense	6,368	26,689	8,596
Net loss	$ (1,154,820)	$ (354,158)	$ (277,746)
Net loss per share attributable to common stockholders, basic and diluted	$ (7.48)	$ (5.84)	$ (4.66)
Weighted-average shares used in computing net loss per share attributable to common stockholders, basic and diluted	154,294	60,628	59,590

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

	Year Ended January 31,		
	2025	2024	2023
	(in thousands)		
Cost of revenue			
Subscription	$ 49,514	$ 45	$ 53
Maintenance	3,076	7	34
Other	14,451	11	140
Research and development	297,051	3,590	3,044
Sales and marketing	330,443	1,313	2,399
General and administrative	219,378	749	1,284
Total stock-based compensation expense	$ 913,913	$ 5,715	$ 6,954

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

	Year Ended January 31,		
	2025	2024	2023
Revenue			
Subscription	93 %	86 %	64 %
Maintenance	3	6	13
Other	4	8	23
Total revenue	100	100	100
Cost of revenue			
Subscription	24	16	10
Maintenance	1	1	3
Other	5	6	17
Total cost of revenue	30	23	30
Gross profit	70	77	70
Operating expenses			
Research and development	60	33	29
Sales and marketing	98	77	71
General and administrative	40	16	14
Total operating expenses	198	126	114
Loss from operations	(128)	(49)	(44)
Interest income	3	2	1
Interest expense	(5)	(5)	(2)
Other income (expense), net	—	—	—
Loss before income taxes	(130)	(52)	(45)
Income tax expense	—	4	1
Net loss	(130)%	(56)%	(46)%

Comparison of Fiscal Years Ended January 31, 2025 and 2024

Revenue

	Year Ended January 31,			
	2025	2024	$ Change	% Change
	(dollars in thousands)			
Revenue				
Subscription	$ 828,740	$ 537,869	$ 290,871	54 %
Maintenance	18,408	38,745	(20,337)	(52)%
Other	39,396	51,278	(11,882)	(23)%
Total revenue	$ 886,544	$ 627,892	$ 258,652	41 %

Growth in subscription revenue was driven by growth in Subscription ARR and modest benefits as customers exercised or forfeited their Subscription Credits but also benefited from the fiscal 2024 revenue headwind related to the transition to RSC and higher than expected upfront and non-recurring revenue. The higher than expected upfront and non-recurring revenue is also due to higher new sales and renewals of RSC-Private from regulated and government verticals in fiscal 2025 as well as the extension of RCDM-T to some of our customers, as they progress through their adoption of RSC.

Our Subscription ARR grew from $784.0 million as of January 31, 2024 to $1,092.6 million as of January 31, 2025, representing a 39% increase. Of the increase in Subscription ARR, 2 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 greater than 120% as of January 31, 2025. We had 2,246 customers with $100,000 or more in Subscription ARR as of January 31, 2025, increasing from 1,742 as of January 31, 2024.

Maintenance revenue associated with sales of perpetual licenses of our legacy CDM product decreased for the fiscal year ended January 31, 2025. Maintenance revenue represented 3% and 6% of total revenue for the fiscal year ended January 31, 2025 and 2024, respectively. We expect the transition of existing maintenance customers adopting RSC subscription offerings to be largely completed by the end of fiscal 2026.

Other revenue, which consists primarily of sales of Rubrik-branded Appliances and professional services, decreased for the fiscal year ended January 31, 2025. Sales of Rubrik-branded Appliances decreased by $10.4 million for the fiscal year ended January 31, 2025, as the transition of sales of our Rubrik-branded Appliances from us to our contract manufacturers is largely complete. We expect our other revenue as a percentage of total revenue to continue to decrease.

Cost of Revenue

	Year Ended January 31,			
	2025	2024	$ Change	% Change
	(dollars in thousands)			
Cost of revenue				
Subscription	$ 215,036	$ 97,927	$ 117,109	120 %
Maintenance	6,068	6,472	(404)	(6)%
Other	44,644	40,563	4,081	10 %
Total cost of revenue	$ 265,748	$ 144,962	$ 120,786	83 %

Cost of subscription revenue increased for the fiscal year ended January 31, 2025 primarily due to the recognition of stock-based compensation expense of $49.5 million after and as a result of the completion of our IPO, an increase in $48.5 million in hosting costs due to the launch and adoption of more SaaS products by our customers, and an increase of $10.6 million from growth in our customer support organization.

Cost of maintenance revenue decreased for the fiscal year ended January 31, 2025 primarily due to $3.1 million decrease in our customer support organization costs relating to maintenance revenue as we no longer offer new perpetual licenses and as existing maintenance customers adopted RSC subscription offerings, offset by an increase of $3.1 million in stock-based compensation expense we recognized after and as a result of the completion of our IPO.

Cost of other revenue increased for the fiscal year ended January 31, 2025 primarily due to $14.5 million in stock-based compensation expense we recognized after and as a result of the completion of our IPO, partially offset by a decrease in Rubrik-branded Appliances costs of $10.9 million as we are transitioning the sale of Rubrik-branded Appliances from us to our contract manufacturers.

Gross Profit and Gross Margin

	Year Ended January 31,			
	2025	2024	$ Change	% Change
	(dollars in thousands)			
Gross profit				
Subscription	$ 613,704	$ 439,942	$ 173,762	39 %
Maintenance	12,340	32,273	(19,933)	(62)%
Other	(5,248)	10,715	(15,963)	(149)%
Total gross profit	$ 620,796	$ 482,930	$ 137,866	29 %

	Year Ended January 31,	
	2025	2024
Gross margin		
Subscription	74 %	82 %
Maintenance	67 %	83 %
Other	(13)%	21 %
Total gross margin	70 %	77 %

Subscription gross margin decreased for the fiscal year ended January 31, 2025 due to the stock-based compensation expense we recognized after and as a result of the completion of our IPO and an increase in hosting costs associated with our development and launch of more SaaS products.

Maintenance gross margin decreased for the fiscal year ended January 31, 2025 due to the stock-based compensation expense we recognized after and as a result of the completion of our IPO.

Other gross margin decreased for the fiscal year ended January 31, 2025 due to the stock-based compensation expense we recognized after and as a result of the completion of our IPO.

Operating Expenses

Research and Development

	Year Ended January 31,			
	2025	2024	$ Change	% Change
	(dollars in thousands)			
Research and development	$ 531,615	$ 206,527	$ 325,088	157 %

Research and development expenses increased for the fiscal year ended January 31, 2025. Employee compensation and related expenses increased by $318.2 million due to $293.5 million of stock-based compensation expense we recognized after and as a result of the completion of our IPO and increases in headcount as we continued to develop new products and enhance the functionalities of our existing products.

Sales and Marketing

	Year Ended January 31,			
	2025	2024	$ Change	% Change
	(dollars in thousands)			
Sales and marketing	$ 867,518	$ 482,532	$ 384,986	80 %

Sales and marketing expenses increased for the fiscal year ended January 31, 2025. Employee compensation and related expenses increased by $366.5 million due to $329.1 million of stock-based compensation expense we recognized after and as a result of the completion of our IPO and increases in headcount.

General and Administrative

	Year Ended January 31,			
	2025	2024	$ Change	% Change
	(dollars in thousands)			
General and administrative	$ 355,695	$ 100,377	$ 255,318	254 %

General and administrative expenses increased for the fiscal year ended January 31, 2025. Employee compensation and related expenses increased by $232.4 million due to $218.6 million of stock-based compensation expense we recognized after and as a result of the completion of our IPO and increases in headcount.

Other Non-Operating Income (Expense)

	Year Ended January 31,			
	2025	2024	$ Change	% Change
	(dollars in thousands)			
Interest income	$ 25,353	$ 11,216	$ 14,137	126 %
Interest expense	(41,253)	(30,295)	(10,958)	36 %
Other income (expense), net	1,480	(1,884)	3,364	(179)%

Interest income increased for the fiscal year ended January 31, 2025 due to higher cash, cash equivalents, and investment balances.

Interest expense increased for the fiscal year ended January 31, 2025 primarily due to our Prior Credit Facility and Amended Credit Facility (each as defined below).

Income Tax Expense

	Year Ended January 31,			
	2025	2024	$ Change	% Change
	(dollars in thousands)			
Income tax expense	$ 6,368	$ 26,689	$ (20,321)	(76)%

Our income tax expense decreased for the fiscal year ended January 31, 2025 due to the impact of integrating the operations of Laminar during the fiscal year ended January 31, 2024 and several of our foreign subsidiaries making an election in the current year to be treated as U.S. branches for federal income tax purposes effective in fiscal 2024.

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

To date, we have financed our operations principally through private placements of our redeemable convertible preferred stock, our term loan credit facility, and payments received from customers. In April 2024, we completed our IPO which resulted in proceeds of approximately $710.3 million, net of underwriting discounts and commissions. In May 2024, our underwriters exercised their option to purchase an additional 3,472,252 shares of our Class A common stock at the IPO Price of $32.00 per share. We received net proceeds of approximately $104.9 million, net of underwriters' discounts and commissions.

In June 2022, we entered into a $195.0 million credit facility (the "Prior Credit Facility"), consisting of initial term loans in an aggregate principal amount of $175.0 million and delayed draw term loan commitments in an aggregate principal amount of $20.0 million. The Prior Credit Facility was scheduled to mature in June 2027. We borrowed the full amount of the initial term loans in June 2022, the proceeds of which were used for general corporate purposes, and subsequently drew approximately $14.5 million of delayed draw term loans to pay accrued quarterly interest payments under the Prior Credit Facility.

In August 2023, we amended and restated the Prior Credit Facility (the "Amended Credit Facility"), to increase the total borrowing capacity thereunder to $330.0 million, consisting of initial term loans in an aggregate principal amount of approximately $289.5 million and delayed draw term loan commitments in an aggregate principal amount of approximately $40.5 million. The Amended Credit Facility will mature in August 2028. We borrowed the full amount of the initial term loans and approximately $4.1 million of delayed draw term loans under the Amended Credit Facility on the closing date of the Amended Credit Facility in order to (i) refinance and replace in full the outstanding term loans under the Prior Credit Facility, (ii) finance the consideration for the acquisition of Laminar, and (iii) pay the accrued quarterly interest under the Prior Credit Facility then due. Borrowings under the Amended Credit Facility will bear interest, at our option, at a rate per annum equal to (i) (x) a base rate equal to the highest of (A) the prime rate as published by The Wall Street Journal, (B) the federal funds rate plus 0.5%, and (C) an adjusted SOFR rate for a one-month interest period plus 1.0% plus (y) a margin of 6.0%, or (ii) an adjusted SOFR rate for a selected interest period plus a margin of 7.0%. We have the option to elect to fund up to 100.0% of the interest payments under the Amended Credit Facility with the incurrence of additional delayed draw term loans, subject to a temporary increase of 0.5% in the annual interest rate due on outstanding term loans for a period of 90 to 180 days from the latest date of incurrence of such additional delayed draw term loans. The annual interest rate on outstanding term loans under the Amended Credit Facility can also decrease by 0.5% if we achieve certain financial targets. In connection with each of the Prior Credit Facility and the Amended Credit Facility, we were also required to pay customary fees for a credit facility of this size and type, including an upfront fee. We have the option to prepay the loans under the Amended Credit Facility at any time subject to a prepayment premium of (i) 1.5% in the first year following the closing of the Amended Credit Facility, (ii) 0.5% in the second year following the closing of the Amended Credit Facility, and (iii) 0.0% thereafter.

In August 2023, we acquired all of the outstanding stock of Laminar, a data security posture management ("DSPM") platform. We accounted for this transaction as a business combination. The acquisition date fair value of the purchase consideration was $104.9 million, of which $90.8 million was paid in cash and the remainder in common stock. The cash consideration of $90.8 million excludes $23.8 million we held back, which is subject to service-based vesting and will be recorded as expense over the period the services are provided. The acquisition of Laminar is intended to support our leadership position as a data security platform provider and help accelerate our cyber posture offerings.

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 or consumption basis based on products purchased due to the growth in our SaaS 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. As of January 31, 2025, we had cash, cash equivalents, and short-term investments of $705.1 million. Our cash equivalents and investments primarily consist of money market funds, 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 $(2,837.3) million as of January 31, 2025. We expect to continue to incur operating losses, and our operating cash flows may fluctuate between positive and negative amounts for the foreseeable future due to the investments we intend to make as described above. As a result, we may require additional capital resources to execute strategic initiatives to grow our business.

We believe that our existing cash and cash equivalents 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 long-term investment balances, and our Amended Credit Facility, 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.

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

	Year Ended January 31,		
	2025	2024	2023
	(in thousands)		
Net cash provided by (used in) operating activities	$ 48,228	$ (4,518)	$ 19,287
Net cash used in investing activities	$ (383,442)	$ (93,623)	$ (125,188)
Net cash provided by financing activities	$ 398,023	$ 95,949	$ 171,823

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 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 from operating activities are for employee compensation and related expenses, sales commissions, fees for third-party professional services, colocation and hosting costs, marketing programs, and discretionary cash payments of our debt interest expense pursuant to the terms of our Amended Credit Facility and prepayments of other spend. 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 fiscal year ended January 31, 2025, net cash provided by operating activities of $48.2 million resulted primarily from a net loss of $1,154.8 million, partially offset by $913.9 million of stock-based compensation, $90.3 million of amortization of deferred commissions, $34.3 million for non-cash interest related to debt, $28.9 million for depreciation and amortization, and $141.7 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 $313.2 million increase in deferred revenue from increased billings and a $45.9 million increase in accrued expenses and other current liabilities. The cash inflow was partially offset by a $128.8 million increase in deferred commissions, a $48.8 million increase in prepaid expense and other assets and a $44.3 million increase in accounts receivable.

For the fiscal year ended January 31, 2024, net cash used in operating activities of $4.5 million resulted primarily from a net loss of $354.2 million, partially offset by $76.5 million of amortization of deferred commissions, $24.3 million for depreciation and amortization, $10.1 million for non-cash interest related to debt, $5.7 million of stock-based compensation, and $233.9 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 $299.8 million increase in deferred revenue from increased billings, a $22.9 million increase in accrued expenses and other liabilities, and a $17.2 million decrease in accounts receivable. The cash inflow was partially offset by a $107.1 million increase in deferred commissions.

Investing Activities

For the fiscal year ended January 31, 2025, net cash used in investing activities of $383.4 million resulted from $797.1 million in purchases of investments, $16.9 million in purchases of property and equipment, and $9.7 million in capitalized internal-use software, offset by $440.3 million in proceeds from maturities and sales of investments.

For the fiscal year ended January 31, 2024, net cash used in investing activities of $93.6 million resulted from $246.0 million in purchases of investments, $90.3 million paid to acquire Laminar, $12.3 million in purchases of property and equipment, and $7.7 million in capitalized internal-use software, offset by $262.7 million in proceeds from maturities and sales of investments.

Financing Activities

For the fiscal year ended January 31, 2025, net cash provided by financing activities of $398.0 million resulted primarily from $815.2 million in proceeds from our IPO and underwriters' exercise of over-allotment option, net of underwriting discounts and commissions, $11.1 million in proceeds from issuance of common stock under employee stock purchase plan, and $8.5 million from the exercise of stock options, partially offset by $432.5 million in taxes paid related to the net share settlement of equity awards that vested since our IPO, and $3.5 million for payment of deferred offering costs.

For the fiscal year ended January 31, 2024, net cash provided by financing activities of $95.9 million resulted primarily from $96.5 million in proceeds from the issuance of debt, net of discount and $3.4 million from the exercise of stock options, offset by $3.7 million for payment of deferred offering costs.

Material Cash Requirements

As of January 31, 2025, our material cash requirements consisted of (i) obligations under operating leases for offices and data centers on an undiscounted basis, of which $11.1 million will be due within 12 months and $19.7 million will be due thereafter, (ii) purchase obligations relating primarily to hosting and software and subscription services, of which $50.0 million will be due within 12 months and $243.2 million will be due thereafter, and (iii) debt, including the quarterly interest payments. As of January 31, 2025, the aggregate principal amount of our $322.3 million debt obligation is due in fiscal 2029.

The contractual commitment amounts above are associated with agreements that are enforceable and legally binding. Obligations under contracts that we can cancel without a significant penalty are not included above. Purchase orders issued in the ordinary course of business are not included above, as our purchase orders represent authorizations to purchase rather than binding agreements.

Critical Accounting Policies and Estimates

Our consolidated financial statements and related notes thereto included elsewhere in this Annual Report on Form 10-K are prepared in accordance with GAAP. The preparation of consolidated financial statements requires us to make estimates and assumptions that affect the reported amounts of assets, liabilities, revenue, and expenses as well as related disclosures. We evaluate our estimates and assumptions on an ongoing basis. Our estimates are based on historical experience and various other assumptions that we believe to be reasonable under the circumstances. Our actual results could differ from these estimates.

The critical accounting estimates, assumptions, and judgments that we believe to have the most significant impact on our consolidated financial statements are described below. Refer to Note 2, Basis of Presentation and Summary of Significant Accounting Policies of the notes to our consolidated financial statements included elsewhere in this Annual Report on Form 10-K for further information on our other significant accounting policies.

Revenue Recognition

We identify 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. We have 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) are provided. In reaching this conclusion, we considered the nature of our promise to customers with a 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. We only fulfill 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.

Our contracts with customers may include customer options that are material rights. The determination of the likelihood of customers exercising their options requires significant judgment. Our management team 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 at 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.

Common Stock Valuations

Prior to the IPO, the fair value of the common stock underlying our stock-based awards has historically been determined by our board of directors, with input from management and reference to contemporaneous unrelated independent third-party valuations. We believe that our board of directors has the relevant experience and expertise to determine the fair value of our common stock. Given the absence of a public trading market of our common stock, and in accordance with the American Institute of Certified Public Accountants Practice Aid, Valuation of Privately-Held-Company Equity Securities Issued as Compensation, our board of directors exercised reasonable judgment and considered numerous objective and subjective factors to determine the best estimate of the fair value of our common stock. These factors include:

- the results of contemporaneous unrelated third-party valuations of our common stock at periodic intervals;
- the prices, rights, preferences, and privileges of our redeemable convertible preferred stock relative to those of its common stock;
- the lack of marketability of our common stock;
- our actual operating and financial results;
- our current business conditions and projections;
- market multiples of comparable companies in our industry;
- the likelihood of achieving a liquidity event, such as an initial public offering or sale of our company, given prevailing market conditions;
- recent secondary stock sales transactions; and
- macroeconomic conditions.

The determination of the fair value of our common stock involves the use of estimates, judgments, and assumptions that are highly complex and subjective, such as those regarding our expected future revenue, expenses, future cash flows, discount rates, market multiples, the selection of comparable public companies, and the probability of and timing associated with possible future events.

Following the IPO, the fair value of our common stock is based on the closing price as reported on the date of grant on the stock exchange on which we are listed.

CEO Performance Award

In June 2022, our board of directors approved a stock option grant to our CEO, Mr. Sinha to purchase up to 8,000,000 shares of Class B common stock. The CEO Performance Award was granted upon our IPO and vests upon the satisfaction of a service-based condition and the achievement of certain stock price goals. We estimated the grant date fair value of the award using the Monte Carlo simulation method which incorporates multiple stock price paths as well as the possibility that the stock price goals may not be satisfied. One of the judgmental assumptions in the Monte Carlo simulation method is the expected volatility of our common stock price. Since we do not have sufficient trading history of our common stock, we estimated the expected volatility at the grant date by using the historical volatility of a group of comparable publicly traded companies over a period equal to the time to expiration of the options.

Recently Issued Accounting Pronouncements

See Note 2, Basis of Presentation and Summary of Significant Accounting Policies, in the notes to our consolidated financial statements included in Part II, Item 8 of this Annual Report on Form 10-K for a discussion of recent accounting pronouncements.

JOBS Act Accounting Election

We are an emerging growth company, as defined in the JOBS Act. The JOBS Act provides that an emerging growth company can take advantage of an extended transition period for complying with new or revised accounting standards. This provision allows an emerging growth company to delay the adoption of some accounting standards until those standards would otherwise apply to private companies. We have elected to use the extended transition period under the JOBS Act for the adoption of certain accounting standards until the earlier of the date we (i) are no longer an emerging growth company or (ii) affirmatively and irrevocably opt out of the extended transition period provided in the JOBS Act. As a result, our financial statements may not be comparable to companies that comply with new or revised accounting pronouncements as of public company effective dates.

Item 7A. 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 January 31, 2025, we had cash, cash equivalents, and short-term investments of $705.1 million and restricted cash of $7.3 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 10% increase or decrease in interest rates would not have a material effect on the fair market value of our portfolio.

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 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 8. Financial Statements and Supplementary Data

Rubrik, Inc.

Index to Consolidated Financial Statements

All other schedules have been omitted because they are not applicable or the required information is shown in the Consolidated Financial Statements or the Notes thereto.

Report of Independent Registered Public Accounting Firm

To the Stockholders and Board of Directors
Rubrik, Inc.:

Opinion on the Consolidated Financial Statements

We have audited the accompanying consolidated balance sheets of Rubrik, Inc. and subsidiaries (the Company) as of January 31, 2025 and 2024, the related consolidated statements of operations, comprehensive loss, redeemable convertible preferred stock and stockholders' deficit, and cash flows for each of the years in the three-year period ended January 31, 2025, and the related notes (collectively, the consolidated financial statements). In our opinion, the consolidated financial statements present fairly, in all material respects, the financial position of the Company as of January 31, 2025 and 2024, and the results of its operations and its cash flows for each of the years in the three-year period ended January 31, 2025, in conformity with U.S. generally accepted accounting principles.

Basis for Opinion

These consolidated financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on these consolidated financial statements based on our audits. We are a public accounting firm registered with the Public Company Accounting Oversight Board (United States) (PCAOB) and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audits in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free of material misstatement, whether due to error or fraud. Our audits included performing procedures to assess the risks of material misstatement of the consolidated financial statements, whether due to error or fraud, and performing procedures that respond to those risks. Such procedures included examining, on a test basis, evidence regarding the amounts and disclosures in the consolidated financial statements. Our audits also included evaluating the accounting principles used and significant estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements. We believe that our audits provide a reasonable basis for our opinion.

/s/ KPMG LLP

We have served as the Company's auditor since 2018.

Santa Clara, California
March 20, 2025

Rubrik, Inc.

CONSOLIDATED BALANCE SHEETS

(in thousands, except share and par value amounts)

	January 31,	
	2025	**2024**
Assets		
Current assets		
Cash and cash equivalents	$ 186,331	$ 130,031
Short-term investments	518,813	149,220
Accounts receivable, net of allowances of $499 and $247	177,627	133,544
Deferred commissions	91,919	72,057
Prepaid expenses and other current assets	102,951	63,861
Total current assets	1,077,641	548,713
Property and equipment, net	53,194	47,873
Deferred commissions, noncurrent	132,465	113,814
Goodwill	100,343	100,343
Other assets, noncurrent	59,331	62,867
Total assets	$ 1,422,974	$ 873,610
Liabilities, redeemable convertible preferred stock and stockholders' deficit		
Current liabilities		
Accounts payable	$ 10,439	$ 6,867
Accrued expenses and other current liabilities	162,602	122,934
Deferred revenue	777,135	526,480
Total current liabilities	950,176	656,281
Deferred revenue, noncurrent	642,370	579,781
Other liabilities, noncurrent	61,821	55,050
Debt, noncurrent	322,341	287,042
Total liabilities	1,976,708	1,578,154
Commitments and contingencies (Note 9)		
Redeemable convertible preferred stock, $0.000025 par value – zero and 74,182,559 shares authorized as of January 31, 2025 and 2024, respectively; zero and 74,182,559 shares issued and outstanding as of January 31, 2025 and 2024, respectively; liquidation preference of zero and $715,100 as of January 31, 2025 and 2024, respectively	—	714,713
Stockholders' deficit		
Preferred stock, $0.000025 par value – 20,000,000 and zero shares authorized as of January 31, 2025 and 2024, respectively; zero shares issued and outstanding as of January 31, 2025 and 2024, respectively	—	—
Common stock, $0.000025 par value – zero and 203,935,682 shares authorized as of January 31, 2025 and 2024, respectively; zero and 55,862,729 shares issued and outstanding as of January 31, 2025 and 2024, respectively	—	1
Convertible founders stock, $0.000125 par value – zero and 5,400,000 shares authorized as of January 31, 2025 and 2024, respectively; zero and 5,400,000 shares issued and outstanding as of January 31, 2025 and 2024, respectively	—	—
Class A common stock, $0.000025 par value – 1,070,000,000 and zero shares authorized as of January 31, 2025 and 2024, respectively; 101,981,023 and zero shares issued and outstanding as of January 31, 2025 and 2024, respectively	3	—
Class B common stock, $0.000025 par value – 210,000,000 and zero shares authorized as of January 31, 2025 and 2024, respectively; 87,785,767 and zero shares issued and outstanding as of January 31, 2025 and 2024, respectively	2	—
Additional paid-in capital	2,291,829	265,494
Accumulated other comprehensive loss	(8,235)	(2,239)
Accumulated deficit	(2,837,333)	(1,682,513)
Total stockholders' deficit	(553,734)	(1,419,257)
Total liabilities, redeemable convertible preferred stock and stockholders' deficit	$ 1,422,974	$ 873,610

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

Rubrik, Inc.

CONSOLIDATED STATEMENTS OF OPERATIONS

(in thousands, except per share amounts)

	Year Ended January 31,		
	2025	**2024**	**2023**
Revenue			
Subscription	$ 828,740	$ 537,869	$ 385,272
Maintenance	18,408	38,745	76,220
Other	39,396	51,278	138,327
Total revenue	886,544	627,892	599,819
Cost of revenue			
Subscription	215,036	97,927	62,294
Maintenance	6,068	6,472	15,059
Other	44,644	40,563	104,661
Total cost of revenue	265,748	144,962	182,014
Gross profit	620,796	482,930	417,805
Operating expenses			
Research and development	531,615	206,527	175,057
Sales and marketing	867,518	482,532	417,542
General and administrative	355,695	100,377	86,754
Total operating expenses	1,754,828	789,436	679,353
Loss from operations	(1,134,032)	(306,506)	(261,548)
Interest income	25,353	11,216	5,140
Interest expense	(41,253)	(30,295)	(11,709)
Other income (expense), net	1,480	(1,884)	(1,033)
Loss before income taxes	(1,148,452)	(327,469)	(269,150)
Income tax expense	6,368	26,689	8,596
Net loss	$ (1,154,820)	$ (354,158)	$ (277,746)
Net loss per share attributable to common stockholders, basic and diluted	$ (7.48)	$ (5.84)	$ (4.66)
Weighted-average shares used in computing net loss per share attributable to common stockholders, basic and diluted	154,294	60,628	59,590

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

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

	Year Ended January 31,		
	2025	2024	2023
Net loss	$ (1,154,820)	$ (354,158)	$ (277,746)
Foreign currency translation adjustment, net of tax	(6,274)	(1,355)	(1,009)
Unrealized gain (loss) on available-for-sale securities, net of tax	278	417	(204)
Total other comprehensive loss, net of tax	(5,996)	(938)	(1,213)
Comprehensive loss	$ (1,160,816)	$ (355,096)	$ (278,959)

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

Rubrik, Inc.

CONSOLIDATED STATEMENTS OF REDEEMABLE CONVERTIBLE PREFERRED STOCK AND STOCKHOLDERS' DEFICIT

(In thousands, except share amounts)

	Redeemable convertible preferred stock		Common stock		Additional paid-in capital	Accumulated other comprehensive income (loss)	Accumulated deficit	Total stockholders' deficit
	Shares	Amount	Shares	Amount				
Balances as of January 31, 2022	74,182,559	$ 714,713	59,156,335	$ 1	$ 231,354	$ (88)	$ (1,050,609)	$ (819,342)
Issuance of common stock upon exercise of stock options	—	—	669,122	—	3,809	—	—	3,809
Repurchases of unvested common stock	—	—	(750)	—	—	—	—	—
Vesting of early exercise stock options	—	—	—	—	164	—	—	164
Issuance of common stock for settlement of restricted stock units	—	—	54,010	—	—	—	—	—
Stock-based compensation	—	—	—	—	6,999	—	—	6,999
Other comprehensive loss	—	—	—	—	—	(1,213)	—	(1,213)
Net loss	—	—	—	—	—	—	(277,746)	(277,746)
Balances as of January 31, 2023	74,182,559	714,713	59,878,717	1	242,326	(1,301)	(1,328,355)	(1,087,329)
Issuance of common stock upon exercise of stock options	—	—	884,012	—	3,383	—	—	3,383
Issuance of common stock for business acquisition	—	—	500,000	—	14,070	—	—	14,070
Stock-based compensation	—	—	—	—	5,715	—	—	5,715
Other comprehensive loss	—	—	—	—	—	(938)	—	(938)
Net loss	—	—	—	—	—	—	(354,158)	(354,158)
Balances as of January 31, 2024	74,182,559	714,713	61,262,729	1	265,494	(2,239)	(1,682,513)	(1,419,257)
Conversion of redeemable convertible preferred stock and founder stock to common stock upon initial public offering	(74,182,559)	(714,713)	74,182,559	2	714,711	—	—	714,713
Issuance of common stock upon initial public offering and underwriters' exercise of over-allotment option, net of underwriting discounts and commissions, and offering costs	—	—	26,972,252	1	805,134	—	—	805,135
Issuance of common stock upon exercise of stock options	—	—	1,548,712	—	8,516	—	—	8,516
Issuance of common stock upon settlement of restricted stock units	—	—	25,393,769	1	(432,513)	—	—	(432,512)
Issuance of common stock under employee stock purchase plan	—	—	406,769	—	11,064	—	—	11,064
Stock-based compensation	—	—	—	—	919,423	—	—	919,423
Other comprehensive loss	—	—	—	—	—	(5,996)	—	(5,996)
Net loss	—	—	—	—	—	—	(1,154,820)	(1,154,820)
Balances as of January 31, 2025	—	$ —	189,766,790	$ 5	$ 2,291,829	$ (8,235)	$ (2,837,333)	$ (553,734)

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

Rubrik, Inc.

CONSOLIDATED STATEMENTS OF CASH FLOWS

(in thousands)

	Year Ended January 31,		
	2025	**2024**	**2023**
Cash flows from operating activities:			
Net loss	$ (1,154,820)	$ (354,158)	$ (277,746)
Adjustments to reconcile net loss to net cash provided by (used in) operating activities:			
Depreciation and amortization	28,868	24,305	22,366
Stock-based compensation	913,913	5,715	6,954
Amortization of deferred commissions	90,303	76,530	81,288
Non-cash interest	34,256	10,117	8,504
Deferred income taxes	1,241	1,937	4,447
Other	(7,249)	(2,836)	(1,034)
Changes in operating assets and liabilities:			
Accounts receivable	(44,255)	17,157	8,754
Deferred commissions	(128,816)	(107,148)	(135,016)
Prepaid expenses and other assets	(48,818)	2,251	(32,702)
Accounts payable	4,479	(1,012)	(7,491)
Accrued expenses and other liabilities	45,882	22,872	2,144
Deferred revenue	313,244	299,752	338,819
Net cash provided by (used in) operating activities	48,228	(4,518)	19,287
Cash flows from investing activities:			
Purchases of property and equipment	(16,885)	(12,333)	(25,017)
Capitalized internal-use software	(9,714)	(7,675)	(9,281)
Purchases of investments	(797,084)	(246,004)	(219,040)
Sale of investments	32,977	7,503	35,910
Maturities of investments	407,264	255,214	92,240
Payment for business combination, net of cash acquired	—	(90,328)	—
Net cash used in investing activities	(383,442)	(93,623)	(125,188)
Cash flows from financing activities:			
Proceeds from initial public offering and underwriters' exercise of over-allotment option, net of underwriting discounts and commissions	815,209	—	—
Taxes paid related to net share settlement of equity awards	(432,512)	—	—
Proceeds from exercise of stock options	8,515	3,383	3,816
Proceeds from issuance of common stock under employee stock purchase plan	11,064	—	—
Repurchases of unvested common stock	—	—	(6)
Payments for deferred offering costs, net	(3,545)	(3,734)	(2,725)
Proceeds from issuance of debt, net of discount	—	96,525	171,463
Payments for debt discount costs	(475)	—	—
Payments for debt issuance costs	(233)	(225)	(725)
Net cash provided by financing activities	398,023	95,949	171,823
Effect of exchange rate on cash, cash equivalents, and restricted cash	(6,274)	(1,355)	(1,009)
Net increase (decrease) in cash, cash equivalents, and restricted cash	56,535	(3,547)	64,913
Cash, cash equivalents, and restricted cash, beginning of year	137,059	140,606	75,693
Cash, cash equivalents, and restricted cash, end of year	$ 193,594	$ 137,059	$ 140,606
Supplemental cash flow information:			
Cash paid for income taxes, net of refunds	$ 11,938	$ 5,054	$ 6,018
Cash paid for interest	15,026	9,518	4,946
Non-cash investing and financing activities:			
Vesting of early exercised common stock options	$ —	$ —	$ 164
Transfers of inventory to property and equipment	$ 102	$ 626	$ 13
Property and equipment received, included in payables and accrued but not paid	$ 816	$ 2,207	$ 1,976
Stock-based compensation capitalized in internal-use software	$ 5,227	$ —	$ 45
Deferred offering costs accrued but not paid	$ —	$ 953	$ 300
Fair value of common stock issued as consideration for business combination	$ —	$ 14,070	$ —

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

Rubrik, Inc.
NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

Note 1 – Description of Business

Rubrik, Inc. (“Rubrik” or the “Company”) is on a mission to secure the world’s data. Rubrik offers data security solutions to organizations ranging from the largest companies worldwide to mid-sized smaller customers. 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.

Initial Public Offering

In April 2024, the Company completed its initial public offering (“IPO”) in which it issued and sold 23,500,000 shares of its Class A common stock at the public offering price of $32.00 per share (the “IPO Price”). The Company received net proceeds of approximately $700.0 million after deducting underwriting discounts and commissions, as well as offering costs.

Immediately prior to the completion of the IPO, all 74,182,559 shares of the Company’s then-outstanding redeemable convertible preferred stock automatically converted into an equal number of shares of Class B common stock, and all 5,400,000 shares of the Company’s then-outstanding convertible founder stock automatically converted into an equal number of shares of Class B common stock.

Prior to the IPO, deferred offering costs, which consist of direct incremental legal, accounting, and other fees relating to the IPO, were capitalized in other assets, noncurrent on the consolidated balance sheets. Upon the consummation of the IPO, $10.3 million of deferred offering costs, net of reimbursement received from the underwriters, were reclassified into stockholders’ equity as an offset against the IPO proceeds.

Prior to the IPO, the Company granted restricted stock units (“RSUs”) with both service-based and liquidity event-related performance-based vesting conditions (“IPO Vesting RSUs”). Upon the consummation of the IPO, the Company recognized stock-based compensation expense for those IPO Vesting RSUs that had met or partially met the service-based vesting condition as the performance-based vesting condition was satisfied. To meet the related tax withholding requirements related to these IPO Vesting RSUs, the Company withheld 12,859,902 shares of Class A common stock subject to the vesting of the IPO Vesting RSUs with a value of $411.5 million to remit to the relevant tax authorities in cash to satisfy such tax obligations as well as any income tax withholding obligations arising as a result of settlement of such shares.

In May 2024, the underwriters exercised their option to purchase an additional 3,472,252 shares of Class A common stock at the IPO Price of $32.00 per share. The Company received net proceeds of approximately $105.1 million after deducting underwriters’ discounts and commissions, as well as offering costs.

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 2025, 2024 and 2023 refer to the fiscal year ending January 31, 2025, 2024 and 2023, respectively.

Basis of Presentation and Principles of Consolidation

The accompanying consolidated financial statements have been prepared in conformity with accounting principles generally accepted in the United States (“U.S. GAAP”). The 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.

Use of Estimates

The preparation of consolidated financial statements in conformity with U.S. GAAP requires management to make estimates and assumptions that affect the amounts reported in the 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 products as well as sales of Rubrik Security Cloud ("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, Enterprise Edition, and Enterprise Proactive 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.

Maintenance revenue

Maintenance revenue represents fees earned from software updates on a when-and-if-available basis, telephone support, integrated web-based support, and Rubrik-branded Appliance support relating to the Company's perpetual licenses. Maintenance revenue is recognized ratably over the term of the service period.

Other revenue

Other revenue represents fees earned from the sale of Rubrik-branded Appliances and professional services.

The Company has determined the Rubrik-branded Appliances and software licenses are separate performance obligations because the Rubrik-branded Appliances and software licenses are not highly interdependent or interrelated and the customer can benefit from the Rubrik-branded Appliances and software licenses separately. The Company does not customize its software licenses and installation services are not required for the software to function.

Rubrik-branded Appliance revenue is recognized when shipped to the customer. The Company's shipping term is free on board shipping point, which means the control of the Rubrik-branded Appliance is transferred to customers upon shipment. When the Company sells software licenses with Rubrik-branded Appliances, revenue related to 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.

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 with Refresh Rights (as defined below) 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)

	Year Ended January 31,		
	2025	2024	2023
Subscription revenue			
Products and services transferred over time	$ 756,660	$ 437,693	$ 219,115
Products and services transferred at a point in time	72,080	100,176	166,157
Maintenance revenue			
Products and services transferred over time	18,408	38,745	76,220
Other revenue			
Products and services transferred over time	29,755	30,728	30,742
Products and services transferred at a point in time	9,641	20,550	107,585
Total revenue	$ 886,544	$ 627,892	$ 599,819

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 consolidated balance sheets. There were $8.5 million and $9.0 million of contract assets as of January 31, 2025 and 2024, respectively. The current and noncurrent contract assets balances as of January 31, 2025 were $4.5 million and $4.0 million, respectively, as of January 31, 2024 were $6.4 million and $2.6 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 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 fiscal years ended January 31, 2025 and 2024, the Company recognized revenue of approximately $535.3 million and $322.5 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 January 31, 2025, total remaining non-cancellable performance obligations under the Company's contracts with customers was approximately $1,811.0 million. The Company expects to recognize approximately 50% of this amount as revenue over the next 12 months, with the remaining balance to be recognized as revenue thereafter.

Cost of Revenue

Cost of revenue primarily consists of salaries, benefits, stock-based compensation, hosting costs, amortization of capitalized internal-use software, amortization of finite-lived intangible assets, and cost of Rubrik-branded Appliances.

Accounts Receivable and Allowances

Accounts receivable is recorded at the invoiced amount, net of allowances. Credit is extended to customers based on an evaluation of their financial condition and other factors. The Company generally does not require collateral or other security to support accounts receivable. The Company performs ongoing credit evaluations of its customers and maintains an allowance, as needed.

These allowances are based on the Company's assessment of the collectibility of accounts by considering the age of the receivable balance, the collection history and type of deals of each customer, and an evaluation of current expected risk of credit loss based on current economic conditions and reasonable and supportable forecasts of future economic conditions over the life of the receivable. The Company assesses collectibility by reviewing accounts receivable and contract assets on an aggregated basis where similar characteristics exist and on an individual basis when the Company identifies specific customers with collectibility issues. Amounts deemed uncollectible are recorded as an allowance in the consolidated balance sheets with a charge to general and administrative expense in the consolidated statements of operations.

The Company presents accrued rebates to Channel Partners on a gross basis in accrued expenses and other current liabilities in the consolidated balance sheets, as the Company's intent is to not settle such amounts net against accounts receivable.

Deferred Commissions

Deferred commissions consist of incremental costs paid to the Company's sales force as a result of acquiring a customer contract. The deferred commission amounts are recoverable through the revenue streams that will be recognized under the related contracts. Sales commissions earned are capitalized using a portfolio approach based on characteristics of historical revenue contracts. Sales commissions are amortized as the related performance obligations are satisfied. Commissions related to performance obligations satisfied over time are amortized over the related period of benefit on a straight-line basis. The related period of benefit is determined to be generally four years when renewal commissions are not commensurate with the initial commissions earned. The Company determines the period of benefit by taking into consideration the length of its customer contracts and the useful life of the underlying products and technology sold. Renewal commissions are deferred and then amortized on a straight-line basis over the contractual term, which is generally one year. Amortization of deferred commissions is included in sales and marketing expense in the consolidated statements of operations. The Company's deferred commissions are classified as current and noncurrent assets within the consolidated balance sheets according to when the Company expects to recognize the expense in the consolidated statement of operations.

Warranties

With respect to the Rubrik-branded Appliance warranty obligation, the Company's contract manufacturer is generally required to replace defective Rubrik-branded Appliances. Furthermore, the Company's customer support agreements provide for the same parts replacement to which customers are entitled under the warranty program, except that replacement parts are delivered according to targeted response times to minimize disruption to the customers' critical business applications. Substantially all customers purchase support agreements.

Given the warranty agreement is with the Company's contract manufacturers and considering that substantially all products are sold together with support agreements, the Company generally has limited exposure related to warranty costs, and therefore no warranty reserve has been recognized for the fiscal years ended January 31, 2025, 2024 and 2023.

Cash, Cash Equivalents, and Restricted Cash

The Company considers cash equivalents to be highly liquid investments with original maturities of three months or less from the date of purchase. Cash equivalents are stated at cost, which approximates fair value.

As of January 31, 2025 and 2024, the Company's restricted cash balance was $7.3 million and $7.0 million, respectively. Restricted cash is included within prepaid expenses and other current assets and other assets, noncurrent on the Company's consolidated balance sheets.

Investments

The Company determines the appropriate classification of its investments at the time of purchase and reevaluates such designation at each balance sheet date. The Company classifies and accounts for its investments as available-for-sale securities as the Company may sell these securities at any time for use in its current operations or for other purposes, even prior to maturity. As a result, the Company classifies its short-term investments, including securities with stated maturities beyond twelve months, within current assets in the consolidated balance sheets.

Available-for-sale securities are recorded at fair value in each reporting period and are periodically evaluated for unrealized losses. For unrealized losses in securities that the Company intends to hold and it is not more likely than not the Company will be required to sell before recovery, the Company further evaluates whether declines in fair value below amortized cost are due to credit or non-credit related factors.

The Company considers credit related impairments to be changes in value that are driven by a change in the creditor's ability to meet its payment obligations, and it records an allowance and recognizes a corresponding loss in other income (expense), net when the impairment is incurred. Unrealized non-credit related losses and unrealized gains are reported as a separate component of accumulated other comprehensive income (loss) in the consolidated balance sheets until realized. Realized gains and losses are determined based on the specific identification method and are reported in other income (expense), net in the consolidated statements of operations.

Fair Value Measurements

Fair value is defined as the price that would be received from selling an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date. When determining the fair value measurements for assets and liabilities that are required to be recorded at fair value, the Company considers the principal or most advantageous market in which to transact and the market-based risk. The Company applies fair value accounting for all assets and liabilities that are recognized or disclosed at fair value in the consolidated financial statements on a recurring basis. The carrying amounts reported in the consolidated financial statements for cash and cash equivalents, accounts receivable, net, accounts payable, and accrued expenses and other current liabilities approximate their fair values due to their short-term nature.

Inventory

Inventory is stated at the lower of cost or net realizable value which approximates actual cost on a first-in, first-out basis.

Property and Equipment

Property and equipment, including leasehold improvements, are stated at cost, net of accumulated depreciation. The Company includes the cost to acquire demonstration units and the related accumulated depreciation in property and equipment, as such units are not available for sale. Depreciation is computed using the straight-line method over the estimated useful lives of the related assets except for leasehold improvements, which are depreciated over the shorter of the useful life of the improvement or the term of the related lease. The useful lives of property and equipment are as follows:

	Useful Lives
Equipment	3 years
Leasehold improvements	Shorter of estimated useful lives of the improvements or remaining related lease term
Furniture and fixtures	5 years

Leases

The Company has entered into non-cancellable operating leases for its offices and data centers with various expiration dates through fiscal year 2031. The Company determines if an arrangement contains a lease at inception based on whether it has the right to control the asset during the contract period and other facts and circumstances. The Company currently does not have any finance leases.

The Company recognizes lease liabilities and right-of-use assets ("ROU assets") at lease commencement. The Company measures lease liabilities based on the present value of future lease payments. The interest rate implicit in the leases is not readily determinable, and therefore the Company uses its incremental borrowing rate based on the information available at the lease commencement date to determine the lease liabilities. The Company does not include in the lease term options to extend or terminate the lease unless it is reasonably certain that the Company will exercise such options. The Company accounts for the lease and non-lease components as a single lease component for its real estate leases. The Company measures the ROU assets based on the corresponding lease liabilities adjusted for prepayments made at or before the lease commencement. The Company does not recognize lease liabilities or ROU assets for short-term leases, which have a lease term of twelve months or less.

The Company begins recognizing operating lease cost on a straight-line basis over the lease term when the lessor makes the underlying asset available to the Company. Variable lease payments are expensed as incurred and are not included in the calculation of lease liabilities or ROU assets.

Software Development Costs

The costs for the development of new software products and substantial enhancements to existing software products are expensed as incurred until technological feasibility has been established, at which time any additional costs are capitalized in accordance with the accounting guidance for software. Because the Company's current process for developing software is essentially completed concurrently with the establishment of technological feasibility, which occurs upon the completion of a working model, no costs have been capitalized for any of the periods presented.

The Company capitalizes certain costs incurred for the development of computer software for internal-use during the application development stage. Costs related to preliminary project activities and post implementation activities are expensed as incurred. Amortization of capitalized internal-use software costs begins when such software is ready for its intended use. Capitalized internal-use software is amortized on a straight-line basis over its estimated useful life of three years. Capitalized internal-use software is included in property and equipment, net in the consolidated balance sheets. The amortization is recorded within subscription cost of revenue in the consolidated statements of operations.

The Company evaluates the useful lives of these assets on an annual basis and tests for impairment whenever events or changes in circumstances occur that could impact the recoverability of these assets.

Research and Development

The Company's research and development expense consists primarily of salaries, benefits, stock-based compensation, third-party infrastructure expenses and depreciation from testing equipment in developing the Company's offerings, and software and subscription services dedicated for use by the Company's research and development organization. Research and development costs that do not meet the software development costs capitalization criteria are expensed as incurred.

Business Combinations

The Company applies the acquisition method of accounting for business combinations under which all assets acquired and liabilities assumed are recorded at their respective fair values at the date of the acquisition.

Any excess of the purchase price over the fair value of the net assets acquired is recognized as goodwill. The Company may record adjustments to the assets acquired and liabilities assumed during the measurement period, which may be up to one year from the acquisition date, with the corresponding offset to goodwill for facts and circumstances that existed as of the acquisition date. Upon the conclusion of the measurement period or final determination of the values of assets acquired or liabilities assumed, whichever comes first, any subsequent adjustments are recorded within the Company's consolidated statements of operations. Acquisition-related costs are recognized separately from the business combination and are expensed as incurred in general and administrative expense in the consolidated statements of operations.

Goodwill and Long-Lived Assets

Goodwill is not amortized but tested for impairment at least annually during the fourth fiscal quarter, or if events or changes in circumstances indicate the carrying amount may no longer be recoverable. The Company operates in one segment, which is considered to be the sole reporting unit, and, therefore, goodwill is tested for impairment at the enterprise level. The Company first evaluates qualitative factors to determine whether it is more likely than not that the fair value of its sole reporting unit is less than its carrying amount. If, as a result of the qualitative assessment, the Company determines that it is more likely than not that the fair value of the reporting unit is more than its carrying amount, then a quantitative goodwill impairment test is not performed. There was no impairment of goodwill for the fiscal years ended January 31, 2025, 2024 and 2023.

Intangible assets, other than the ones with indefinite useful lives, are carried at cost, net of accumulated amortization. Amortization is recorded on a straight-line basis over the intangible assets' useful lives. Intangible assets, net is included within other assets, noncurrent on the Company's consolidated balance sheets.

Long-lived assets, such as property and equipment and finite-lived intangible assets, are subject to amortization and reviewed for impairment whenever events or changes in circumstances indicate that the carrying value may not be recoverable. Recoverability is measured by comparing the net book value to the future undiscounted cash flows attributable to such assets. If impaired, the Company recognizes an impairment charge equal to the amount by which the net book value exceeds its fair value. There was no impairment charge of long-lived assets for the fiscal years ended January 31, 2025, 2024 and 2023, respectively.

Advertising Costs

Advertising costs are expensed as incurred in sales and marketing expense in the consolidated statements of operations and amounted to $35.6 million, $31.3 million and $33.3 million for the fiscal years ended January 31, 2025, 2024 and 2023, respectively.

Stock-Based Compensation Expense

The Company measures and recognizes stock-based compensation expense for all equity awards made to employees, nonemployees, and the Company's board of directors (the "Board of Directors"), and stock purchase rights granted under the Employee Stock Purchase Plan ("ESPP") to employees based on estimated fair values at the date of grant.

The Company estimates the fair value of its options and ESPP rights using the Black-Scholes option pricing model which requires the input of assumptions. These assumptions and estimates are as follows:

Fair value of common stock — Prior to the Company's IPO, the Company estimated the fair value of common stock as the Company's common stock was not yet publicly traded. The Board of Directors considered numerous objective and subjective factors to determine the fair value of the Company's common stock at each meeting in which awards were approved. The factors considered included, but were not limited to: (i) the results of contemporaneous unrelated third-party valuations of the Company's common stock, (ii) the prices, rights, preferences and privileges of the Company's Preferred Stock relative to those of its common stock, (iii) the lack of marketability of the Company's common stock, (iv) actual operating and financial results, (v) current business conditions and projections, (vi) market multiples of comparable companies in the Company's industry, (vii) the likelihood of achieving a liquidity event, such as an initial public offering or sale of the Company, given prevailing market conditions, (viii) recent secondary stock sales transactions, and (ix) macroeconomic conditions. After the completion of the IPO, the fair value of each share of the underlying common stock is based on the closing price of our Class A common stock as reported on the New York Stock Exchange on the date of the grant.

Expected term — The Company determines the expected term based on the average period the stock options are expected to remain outstanding, generally calculated as the midpoint of the stock option's vesting term and contractual expiration period, as the Company does not have sufficient historical information to develop reasonable expectations about future exercise patterns and post-vesting employment termination behavior.

Expected volatility — Expected volatility is a measure of the amount by which the stock price is expected to fluctuate. Since the Company does not have sufficient trading history of its common stock, it estimates the expected volatility of its stock options at their grant date by taking the weighted-average historical volatility of a group of comparable publicly traded companies over a period equal to the expected term of the options.

Risk-free interest rate — The Company uses the U.S. Treasury yield in effect at the time of grant for the expected term of the stock options issued.

Dividend yield — The Company utilizes a dividend yield of zero, as it does not currently issue dividends and does not expect to in the future.

The Company granted RSUs that vest upon satisfaction of a service-based condition only and also those that have both a service-based condition and a performance-based condition. The grant-date fair value of these RSUs is the fair value of the Company's common stock on the date of grant.

The grant-date fair value of equity awards which include a market-based condition is estimated using the Monte Carlo simulation method which incorporates the possibility that the market-based condition may not be satisfied, and various assumptions including expected term, expected volatility, and risk-free interest rates.

The Company recognizes stock-based compensation expense on a straight-line basis over the requisite service period for equity awards with service-based conditions only. Stock-based compensation expense for equity awards with a service-based condition and a performance-based condition or a market-based condition, or both, will be recognized using the accelerated attribution method over the requisite service period. For equity awards of which vesting conditions include a market-based condition, the stock-based compensation expense is recognized using the accelerated attribution method over the requisite service period, regardless of whether the market-based condition is met.

Stock-based compensation expense is not recognized for grants that include a performance-based condition until the performance-based condition is deemed probable. A performance-based condition could be the occurrence of a qualifying event. A qualifying event is defined as (i) immediately prior to a sale event, as defined in the Company's 2014 Stock Option and Grant Plan (the "2014 Plan"), or (ii) the Company's IPO, as defined in the 2014 Plan, in either case, occurring prior to the expiration date. In the period in which the qualifying event becomes probable, the Company will record cumulative stock-based compensation expense for those RSUs for which the service-based condition has been satisfied or partially satisfied. Stock-based compensation related to any remaining service-based conditions after the qualifying event-related performance condition is satisfied will be recorded over the remaining requisite service period.

Forfeitures are accounted for as they occur.

Foreign Currency

The functional currency of the Company's foreign subsidiaries is the respective local currency. Translation adjustments arising from the use of differing exchange rates from period to period are included in accumulated other comprehensive loss in the consolidated balance sheets. Foreign currency transaction gains and losses are included in other income (expense), net in the consolidated statements of operations. Revenue and expenses are translated at the average exchange rate during the period, and equity balances are translated using historical exchange rates. To date, the Company has not undertaken any hedging transactions related to foreign currency exposure.

Income Taxes

The Company accounts for income taxes using the asset and liability method. Under this method, the Company recognizes deferred tax assets and liabilities for the expected future tax consequences of temporary differences between the financial reporting and tax basis of assets and liabilities, as well as for net operating loss and tax credit carryforwards. Deferred tax assets and liabilities are measured using enacted tax rates that are expected to apply to taxable income for the years in which those tax assets and liabilities are expected to be realized or settled. The measurement of deferred tax assets is reduced, if necessary, by a valuation allowance to amounts that are more likely than not to be realized.

The Company records a liability for uncertain tax positions if it is not more likely than not to be sustained based solely on its technical merits as of the reporting date. The Company considers many factors when evaluating and estimating its tax positions and tax benefits.

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 credit losses as of January 31, 2025.

Concentration of revenue and accounts receivable

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

	Revenue			Accounts Receivable, Net	
	Year Ended January 31,			January 31,	
	2025	2024	2023	2025	2024
Partner A	29%	30%	32 %	33%	44%
Partner B	34%	35%	35 %	20%	25%
Partner C	10%	11%	12 %	14%	*

* 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.

The Company relies on a limited number of suppliers for its contract manufacturing and certain raw material components. In instances where suppliers fail to perform their obligations, the Company may be unable to find alternative suppliers or satisfactorily deliver its products to its customers on time.

Net Loss Per Share

The Company computes basic and diluted net loss per share attributable to Class A and Class B common stockholders for the fiscal year ended January 31, 2025 and basic and diluted net loss per share attributable to common and convertible founder stockholders for the fiscal years ended January 31, 2024 and 2023 using the two-class method required for companies with participating securities. The Company considered all series of its redeemable convertible preferred stock to be participating securities as the holders of the redeemable convertible preferred stock were entitled to receive a non-cumulative dividend on a pari passu basis in the event that a dividend is paid on the common stock. Under the two-class method, the net loss attributable to common stockholders was not allocated to the redeemable convertible preferred stock as the preferred stockholders did not have a contractual obligation to share in the Company's losses.

Basic net loss per share attributable to common stockholders is computed by dividing the net loss attributable to common stockholders by the weighted-average number of shares of common stock outstanding during the period. Diluted net loss per share is computed by giving effect to all potential shares of common stock, including redeemable convertible preferred stock, issued and outstanding common stock options, unvested RSUs issued and outstanding, and ESPP, to the extent they are dilutive.

Recent Accounting Pronouncements

Recently Adopted Accounting Pronouncements

In November 2023, the Financial Accounting Standards Board ("FASB") issued Accounting Standards Update ("ASU") 2023-07, Improvements to Reportable Segment Disclosures, which updates reportable segment disclosure requirements primarily through enhanced disclosures about significant segment expenses. The guidance is effective for the Company's annual report for its fiscal year beginning February 1, 2024 and interim periods within its fiscal year beginning February 1, 2025, on a retrospective basis. Early adoption is permitted. The Company adopted ASU 2023-07 in the fourth quarter of the fiscal year ended January 31, 2025. See Note 14 Segment Reporting.

Recently Announced Accounting Pronouncements Not Yet Adopted

In December 2023, the FASB issued ASU 2023-09, Improvements to Income Tax Disclosures, which requires entities to provide consistent categories and greater disaggregation of information in the rate reconciliation as well as income tax paid disaggregated by jurisdiction to improve the transparency of income tax disclosures. ASU 2023-09 is effective for annual periods beginning after December 15, 2024, on a prospective basis, with early adoption permitted. The Company is assessing the timing and impact of adopting this standard.

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.

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):

	Year Ended January 31,		
	2025	2024	2023
Americas	$ 636,191	$ 441,537	$ 428,304
EMEA	214,098	162,161	149,853
APAC	36,255	24,194	21,662
Total revenue	$ 886,544	$ 627,892	$ 599,819

For the fiscal years ended January 31, 2025, 2024 and 2023, United States accounted for $612.9 million, $427.0 million and $416.1 million, respectively, or 69%, 68% and 69%, respectively, of consolidated total revenue.

Note 4 – Business Combinations

In August 2023, the Company acquired all outstanding stock of Laminar Technologies, Inc. ("Laminar"), a data security posture management platform. The Company accounted for this transaction as a business combination. The acquisition date fair value of the purchase consideration was $104.9 million, of which $90.8 million was paid in cash and the remainder in common stock. The cash consideration of $90.8 million excludes $23.8 million held back by the Company, which is subject to service-based vesting and will be recorded as expense over the period the services are provided. The acquisition of Laminar is to support Rubrik's leadership position as a data security platform provider and help accelerate the Company's cyber posture offerings. The Company recorded $11.0 million as an acquired developed technology intangible asset with an estimated useful life of three years and $96.1 million of goodwill which is primarily attributed to assembled workforce as well as the integration of Laminar's technology with the Company's technology. The goodwill is not deductible for tax purposes. The remaining assets acquired and liabilities assumed on the acquisition date were not material.

Pro forma results of operations for the business combination have not been presented, as they were not material to the consolidated statements of operations. Acquisition-related costs for the business combination were expensed as incurred within general and administrative expense in the consolidated statements of operations and were not material.

The Company recognized $3.7 million, $1.7 million and $0.8 million amortization expense in acquired intangible assets for the fiscal years ended January 31, 2025, 2024 and 2023, respectively.

Note 5 – 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.
- 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 judgement or estimation.

The Company did not have any level 3 investments as of January 31, 2025 and 2024. 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):

					Reported as	
January 31, 2025	Amortized Cost	Gross Unrealized Gains	Gross Unrealized Losses	Estimated Fair Value	Cash and Cash Equivalents	Short-Term Investments
Cash:	$ 75,541	$ —	$ —	$ 75,541	$ 75,541	$ —
Level 1:						
Money market funds	96,423	—	—	96,423	96,423	—
U.S. Treasuries	259,327	345	(76)	259,596	—	259,596
Subtotal	355,750	345	(76)	356,019	96,423	259,596
Level 2:						
Commercial paper	88,732	8	(3)	88,737	14,367	74,370
Corporate bonds	184,742	195	(90)	184,847	—	184,847
Subtotal	273,474	203	(93)	273,584	14,367	259,217
Total	$ 704,765	$ 548	$ (169)	$ 705,144	$ 186,331	$ 518,813

January 31, 2024	Amortized Cost	Gross Unrealized Gains	Gross Unrealized Losses	Estimated Fair Value	Reported as	
					Cash and Cash Equivalents	Short-Term Investments
Cash:	$ 72,420	$ —	$ —	$ 72,420	$ 72,420	$ —
Level 1:						
Money market funds	47,696	—	—	47,696	47,696	—
U.S. Treasuries	86,429	70	(13)	86,486	—	86,486
Subtotal	134,125	70	(13)	134,182	47,696	86,486
Level 2:						
Commercial paper	33,019	3	(3)	33,019	9,915	23,104
Corporate bonds	17,883	30	(3)	17,910	—	17,910
U.S. government agencies	21,703	27	(10)	21,720	—	21,720
Subtotal	72,605	60	(16)	72,649	9,915	62,734
Total	$ 279,150	$ 130	$ (29)	$ 279,251	$ 130,031	$ 149,220

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

	January 31, 2025
Due within one year	$ 448,397
Due between one to two years	70,416
Total	$ 518,813

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 January 31, 2025 and 2024.

Note 6 – Balance Sheet Components

Prepaid Expenses and Other Current Assets

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

	January 31,	
	2025	2024
Prepaid expenses	$ 77,857	$ 44,721
Inventory, net	4,183	4,807
Contract assets, current	4,537	6,356
Other current assets	16,374	7,977
Total prepaid expenses and other current assets	$ 102,951	$ 63,861

Property and Equipment, Net

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

	January 31,	
	2025	2024
Equipment	$ 75,589	$ 91,645
Capitalized internal-use software	36,132	21,191
Leasehold improvements	12,739	12,350
Furniture and fixtures	4,687	4,150
Total property and equipment, gross	129,147	129,336
Less: accumulated depreciation and amortization	(75,953)	(81,463)
Total property and equipment, net	$ 53,194	$ 47,873

Depreciation expense related to the Company's property and equipment, which did not include amortization expense related to capitalized internal-use software, was $17.4 million, $16.7 million and $15.5 million for the fiscal years ended January 31, 2025, 2024 and 2023, respectively.

Amortization expense relating to capitalized internal-use software was $7.8 million, $5.9 million and $6.1 million for the fiscal years ended January 31, 2025, 2024 and 2023, respectively.

Accrued Expenses and Other Current Liabilities

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

	January 31,	
	2025	2024
Accrued expenses	$ 30,983	$ 41,773
Accrued bonuses	49,104	31,212
Accrued sales commissions	27,627	18,859
Accrued payroll-related expenses, taxes, and benefits	38,533	20,197
Operating lease liabilities	10,087	10,461
Other	6,268	432
Total accrued expenses and other current liabilities	$ 162,602	$ 122,934

Note 7 – Leases

The Company has operating leases for its offices and data centers. Balance sheet information related to operating leases was as follows (in thousands):

	January 31,	
Reported as:	2025	2024
Other assets, noncurrent (operating lease ROU assets)	$ 25,906	$ 29,833
Accrued expenses and other current liabilities (operating lease liabilities, current)	10,087	10,461
Other liabilities, noncurrent (operating lease liabilities, noncurrent)	18,382	22,252
Total operating lease liabilities	$ 28,469	$ 32,713

The Company had operating lease costs of $11.9 million, $11.1 million and $10.3 million for the fiscal years ended January 31, 2025, 2024 and 2023, respectively.

Supplemental cash flow information and non-cash activity related to the Company's operating leases were as follows (in thousands):

	Year Ended January 31,		
	2025	2024	2023
Cash paid for amounts included in measurement of operating lease liabilities	$ 12,261	$ 11,397	$ 10,244
ROU assets obtained in exchange of lease liabilities for new operating leases	$ 6,810	$ 6,375	$ 11,969

Supplemental information related to the remaining lease term and discount rate were as follows:

	January 31,	
	2025	2024
Weighted-average remaining lease term	3.0 years	3.6 years
Weighted-average discount rate	5.5%	5.1%

The following table summarizes the maturity of the Company's operating lease liabilities as of January 31, 2025 (in thousands):

Fiscal Year Ending January 31,	Operating Leases
2026	$ 11,103
2027	9,552
2028	8,218
2029	1,445
2030	449
Thereafter	—
Total operating lease payments	30,767
Less: imputed interest	(2,298)
Total operating lease liabilities	$ 28,469

Note 8 – Debt

Term Loan

In June 2022, the Company entered into a credit agreement with a consortium of lenders for a total $195.0 million revolving credit facility (the "Prior Credit Facility") consisting of a $175.0 million term loan (the "Prior Closing Date Term Loan") and $20.0 million in committed delayed-draw term loans (the "Prior Delayed Draw Term Loans") with a maturity date of June 10, 2027. The proceeds of the Prior Delayed Draw Term Loans were to be used to pay accrued interest relating to the Prior Credit Facility. The Company also had the option to request incremental Delayed Draw Term Loan commitments (the "Prior Supplemental Delayed Draw Term Loans" and, together with the Prior Delayed Draw Term Loans and the Prior Closing Date Term Loan, collectively, the "Prior Loans"). The terms of the Prior Supplemental Delayed Draw Term Loans were identical to the Prior Delayed Draw Term Loans. The Company borrowed the full $175.0 million Prior Closing Date Term Loan with a closing date of June 10, 2022 and incurred $4.3 million debt discount and issuance costs.

Under the Prior Credit Facility, interest accrued on the Prior Loans, at the Company's election made at the time of borrowing, at either the Alternate Base Rate ("ABR") or Secured Overnight Financing Rate ("SOFR"). The Company also had the option to convert all or a portion of the outstanding principal amount to/from a SOFR-based loan to/from an ABR-based loan after the initial election. ABR loans had an annual interest rate equal to ABR plus 5.5%. ABR is a fluctuating interest rate per annum equal to the highest of: (i) prime rate, (ii) federal funds rate plus 0.5%, or (iii) Term SOFR for one month plus 1.0%. SOFR loans had an annual interest rate equal to Term SOFR plus 6.5%. Term SOFR is a rate per annum equal to the greater of: (i) the floor of 1.0% or (ii) the sum of Term SOFR Reference Rate plus Term SOFR Adjustment applicable to the comparable Interest Period (as defined in the June 2022 credit agreement). The Company had the option to elect an Interest Period of one, three, or six months on the SOFR loans as long as the election did not extend beyond the maturity date of June 10, 2027. The annual interest rate was subject to a 0.5% increase and separately, a 0.5% decrease depending on certain actions by the Company.

Interest on ABR loans was payable quarterly in arrears. Interest on SOFR loans was payable on the last day of each Interest Period, but if the interest period was more than three months, interest was payable on the last day of each three-month interval after the first day of such Interest Period.

In August 2023, the Company executed an amended and restated credit agreement with a consortium of lenders for a total $330.0 million revolving credit facility (the "Amended Credit Facility") consisting of a $289.5 million term loan (the "Amended Term Loan") and $40.5 million in committed delayed draw term loan (the "Amended Delayed Draw Term Loan") with a maturity date of August 17, 2028. The Amended Credit Facility replaced the Prior Credit Facility. Immediately prior to the closing date of the Amended Credit Facility, the Company had an outstanding balance under the Prior Credit Facility of $193.6 million which consisted of $189.5 million of the Prior Loans and $4.1 million of unpaid interest under the Prior Credit Facility. The Company borrowed the full $289.5 million Amended Term Loan and used a portion to replace and refinance the full $189.5 million of the Prior Loans. The Company borrowed $4.1 million under the Amended Delayed Draw Term Loan to fund the unpaid interest under the Prior Credit Facility. The Company incurred $3.5 million debt discount costs in relation to the Amended Credit Facility.

The interest terms under the Amended Credit Facility are identical to the interest terms under the Prior Credit Facility except the ABR loan has an annual interest rate equal to ABR plus 6.0%, the SOFR loan has an annual interest rate equal to Term SOFR plus 7.0%, and the maturity date is August 17, 2028.

Under the Amended Credit Facility, the prepayment starts at 1.5% and reduces to zero beginning on the third anniversary from the closing date. Any amounts drawn and repaid or prepaid under the Amended Credit Facility may not be reborrowed.

The Company will have the option to fund up to 100.0% of cash interest with the proceeds of the Amended Delayed Draw Term Loan, subject to a 0.5% increase in the annual interest rate effective from the date of funding for 90 days, or 180 days if the Interest Period for such Amended Delayed Draw Term Loan is six months from the date of funding.

Under the Amended Credit Facility, the annual interest rate on all outstanding principal amounts will be reduced by 0.5% if the Company's Annualized Subscription Recurring Revenue (as defined in the amended credit agreement, "ASRR") is at least $500.0 million and the Company delivers a compliance certificate in accordance with the amended credit agreement.

The amended credit agreement contains certain covenants that require the Company, among other things, to maintain a specified minimum liquidity amount and minimum ASRR amount. Failure to comply with these covenants, along with other non-financial covenants, could result in an event of default, which may lead to acceleration of the amounts owed and/or the enforcement of other remedies by the lenders.

The Company had $6.9 million of debt discount and issuance costs on the $293.6 million Amended Term Loan and Amended Delayed Draw Term Loan as of August 17, 2023. The debt discount and issuance costs were recorded as a direct deduction from the long-term debt liability and are amortized into interest expense over the contractual term of the Amended Credit Facility.

Under the Amended Delayed Draw Term Loan, the Company borrowed $34.3 million and $4.1 million for the fiscal years ended January 31, 2025 and 2024, respectively.

As of January 31, 2025 and 2024, the Company was in compliance with all of its debt covenants.

Bridge Notes

In April 2024, the Company entered into a purchase agreement with Goldman Sachs & Co. LLC and Barclays Capital Inc. (collectively, the "Purchasers") for the Company to issue senior notes (the "Bridge Notes") to the Purchasers for up to $450.0 million. The Company issued the Bridge Notes and received the funding from the Purchasers on April 25, 2024 (the "Funding Date") in an aggregate amount of $321.4 million to fund a portion of the tax withholding and remittance obligations related to the settlement of RSUs in connection with the IPO. The Bridge Notes matured on April 29, 2024 (the "IPO Settlement Date") and carried an annual interest rate of 7.0% starting from the Funding Date up to but excluding the date of repayment.

The Company incurred $0.6 million of discount and issuance costs in connection with the issuance of Bridge Notes and recorded it as a direct deduction from the Bridge Notes liability on the date of issuance.

On April 29, 2024, the Company repaid the outstanding principal amount of the Bridge Notes, including $0.2 million of accrued and unpaid interest which was recorded as interest expense. The aggregate unamortized amount of discount and issuance costs was fully amortized into interest expense for the three months ended April 30, 2024.

Note 9 – Commitments and Contingencies

Purchase Commitments

In December 2024, the Company entered into three-year contracts with certain third-parties for hosting services. The Company is required to spend a minimum of $200.0 million over the term of the contracts. As of January 31, 2025, the Company had $178.7 million remaining on these commitments.

In addition to the commitments described above, as of January 31, 2025, the Company had other remaining purchase commitments of approximately $114.5 million primarily for hosting costs and software and subscription services.

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 consolidated balance sheets, consolidated statements of operations, or consolidated statements of 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 10 – Redeemable Convertible Preferred Stock

Immediately prior to the closing of the IPO, all 74,182,559 shares of the Company's redeemable convertible preferred stock outstanding were automatically converted into an equivalent number of shares of Class B common stock on a one-to-one basis, and their carrying value of $714.7 million was reclassified into stockholders' equity. As of January 31, 2025, there were no shares of redeemable convertible preferred stock issued and outstanding.

The authorized, issued and outstanding shares of redeemable convertible preferred stock and liquidation preferences as of January 31, 2024 were as follows (in thousands, except share amounts):

	Authorized Shares	Issued and Outstanding Shares	Liquidation Preference	Carrying Value
Series A	15,255,884	15,255,884	$ 10,255	$ 10,229
Series B	16,751,780	16,751,780	41,000	40,974
Series C	8,937,037	8,937,037	61,250	61,187
Series D	15,406,551	15,406,551	182,600	182,505
Series E	17,831,307	17,831,307	419,995	419,818
	74,182,559	74,182,559	$ 715,100	$ 714,713

The holders of shares of Preferred Stock had various rights and preferences.

Dividends

The holders of shares of Preferred Stock were entitled to receive noncumulative dividends at the specified dividend rate of $0.053775 per annum for each share of Series A Preferred Stock ("Series A"), $0.1958 per annum for each share of Series B Preferred Stock ("Series B"), $0.5483 per annum for each share of Series C Preferred Stock ("Series C"), $0.9482 per annum for each share of Series D Preferred Stock ("Series D"), and $1.8843 per annum for each share of Series E Preferred Stock ("Series E"), if and when declared by the Board of the Directors. Dividends to holders of Series A, Series B, Series C, Series D and Series E were to be paid in advance of any distributions on Founders Stock and Common Stock.

No dividends have been declared to date.

Liquidation

In the event of a liquidation event, either voluntary or involuntary, the holders of each series of Preferred Stock would have been entitled to receive on a pari passu basis out of the proceeds of assets of the Company available for distribution the greater of (i) an amount equal to the sum of (a) the original issue price, as follows: $0.6722 per share for each share of Series A, $2.4475 per share for each share of Series B, $6.8535 per share for each share of Series C, $11.8521 per share for each share of Series D, $23.5538 per share for each share of Series E, and (b) declared but unpaid dividends on such share or (ii) the amount per share that would be payable had all shares of such series of Preferred Stock been converted into Common Stock immediately prior to such Liquidation Event.

Redemption

The holders of Preferred Stock had no voluntary rights to redeem their shares. The Preferred Stock had deemed liquidation provisions which required the shares to be redeemed upon a change in control or other deemed liquidation events. Although the Preferred Stock was not mandatorily or currently redeemable, a deemed liquidation event would constitute a redemption event outside the Company's control. As a result of these liquidation features, all shares of Preferred Stock were classified outside of stockholders' deficit on the consolidated balance sheets. The carrying values of the Company's Preferred Stock had not been accreted to their redemption values as these events were not considered probable of occurring. Subsequent adjustments of the carrying values to redemption values would be made only if and when it becomes probable the preferred shares will become redeemable.

Conversion

Each share of Series A, Series B, Series C, Series D and Series E was convertible into Common Stock at any time at the option of the stockholder by dividing $0.6722, $2.4475, $6.8535, $11.8521 and $23.5538, respectively (the original issue price per share, split adjusted) by the applicable conversion price. The initial conversion price per share for Series A, Series B, Series C, Series D and Series E was $0.6722, $2.4475, $6.8535, $11.8521 and $23.5538, respectively. The conversion price would have been subject to adjustments as set forth in the Company's amended and restated certificate of incorporation upon the occurrence of certain events, such as stock splits and stock dividends. Each share of Preferred Stock would have been automatically converted into shares of Common Stock immediately upon the earlier of (i) closing of the Company's sale of the Company's Common Stock in a firm commitment underwritten public offering pursuant to a registration statement on Form S-1 under the Securities Act of 1933, as amended, with an aggregate offering price to the public of at least $35 million or (ii) the date, or the occurrence of an event, specified by vote or written consent or agreement of the holders of a majority of the then outstanding shares of Preferred Stock.

Voting

Each holder of shares of Preferred Stock was entitled to voting rights equivalent to the number of shares of Common Stock into which the respective shares were convertible. Certain transactions required the vote of at least a majority of outstanding shares of Series B, 60% of outstanding shares of Series C, a majority of outstanding shares of Series D, a majority of outstanding shares of Series E, or the holders of majority of the shares of outstanding Preferred Stock.

Note 11 – Stockholders' Deficit

Preferred Stock

In connection with the IPO, the Company's amended and restated certificate of incorporation became effective, which authorized the issuance of 20,000,000 shares of undesignated preferred stock with a par value of $0.000025 per share with rights and preferences, including voting rights, designated from time to time by the board of directors.

Common Stock

The Company has two classes of common stock – Class A common stock and Class B common stock. In connection with the IPO, the Company's amended and restated certificate of incorporation authorized the issuance of 1,070,000,000 shares of Class A common stock and 210,000,000 shares of Class B common stock. The shares of Class A common stock and Class B common stock are identical, except with respect to voting, conversion, and transfer rights. Each share of Class A common stock is entitled to one vote. Each share of Class B common stock is entitled to 20 votes. Class A and Class B common stock have a par value of $0.000025 per share, and are referred to collectively as common stock throughout the notes to the consolidated financial statements, unless otherwise noted. Holders of common stock are entitled to receive any dividends as may be declared from time to time by the board of directors.

Each share of Class B common stock is convertible at any time at the option of the holder into one share of Class A common stock. Any holder's shares of Class B common stock will convert automatically to Class A common stock, on a one-to-one basis, upon the earliest to occur following the Company's IPO: (i) sale or transfer of such share of Class B common stock, except for permitted transfers as described in the amended and restated certificate of incorporation; (ii) the death or incapacity of the Class B common stockholder (or 180 days following the date of the death or incapacity if the stockholder is one of the Company's founders); and (iii) on the final conversion date, defined as the earliest of (a) the date fixed by the Company's board of directors that is no less than 61 days and no more than 180 days following the date on which the outstanding shares of Class B common stock represent less than 5% of the then outstanding shares of Class A and Class B common stock; (b) the last trading day of the fiscal year following the tenth anniversary of the effectiveness of the registration statement in connection with the Company's IPO; (c) the date fixed by the Company's board of directors that is no less than 61 days and no more than 180 days following the date that Bipul Sinha is no longer providing services to the Company as an officer, employee, or director; (d) the date fixed by the board of directors that is no less than 61 days and no more than 180 days following the death or incapacity of Mr. Sinha; or (e) the date specified by a vote of the holders of a majority of the outstanding shares of Class B common stock.

Immediately prior to the closing of the IPO, all 5,400,000 shares of the Company's convertible founder stock outstanding were automatically converted into an equal number of shares of Class B common stock. As of January 31, 2025, there were no shares of convertible founder stock issued and outstanding.

Equity Incentive Plan

In January 2014, the Company adopted the 2014 Stock Option and Grant Plan, as amended (the "2014 Plan"). The 2014 Plan permits the grant of incentive stock options, non-qualified stock options, restricted stock awards, unrestricted stock awards, or RSU awards based on, or related to, shares of the Company's common stock. The 2014 Plan was terminated in April 2024 in connection with the IPO, but continues to govern the terms of outstanding awards that were granted prior to the termination of the 2014 Plan. No further equity awards will be granted under the 2014 Plan. With the establishment of the 2024 Equity Incentive Plan (the "2024 Plan"), upon the expiration, forfeiture, cancellation, or reacquisition of any shares of Class B common stock underlying outstanding equity awards granted under the 2014 Plan, an equal number of shares of Class A common stock will become available for grant under the 2024 Plan.

In March 2024, the Company's board of directors adopted, and in April 2024, the Company's stockholders approved, the 2024 Plan, which became effective in connection with the Company's IPO. The 2024 Plan provides for the grant of incentive stock options, nonqualified stock options, stock appreciation rights, restricted stock awards, RSU awards, performance-based awards, and other forms of awards to employees, non-employee directors and consultants, and employees and consultants of the Company's affiliates. A total of 46,073,027 shares of the Company's Class A common stock have been reserved for future issuance under the 2024 Plan in addition to (i) shares underlying outstanding equity awards granted under the 2014 Plan that expire, or are forfeited, cancelled, or reacquired, as described above, and (ii) any automatic increases in the number of shares of Class A common stock reserved for future issuance under this plan.

In March 2024, the board of directors adopted, and in April 2024, the stockholders approved, the 2024 Employee Stock Purchase Plan (the "2024 ESPP" or the "ESPP"), which became effective in connection with the Company's IPO. The 2024 ESPP authorizes the issuance of shares of Class A common stock pursuant to purchase rights granted to employees. A total of 4,607,303 shares of the Company's Class A common stock have been reserved for future issuance under the 2024 ESPP. The number of shares of Class A common stock reserved for issuance under the 2024 ESPP will automatically increase on February 1 of each fiscal year, beginning on February 1, 2025 and ending on and including February 1, 2034, by the lesser of (1) one percent (1%) of the aggregate number of shares of common stock of all classes issued and outstanding on January 31 of the preceding fiscal year, (2) 9,214,605 shares, or (3) a lesser number of shares determined by the Company's board of directors.

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

	January 31,	
	2025	2024
Conversion of Preferred Stock	—	74,183
Conversion of Founders Stock	—	5,400
2014 Stock Option and Grant Plan:		
Outstanding stock options	9,570	3,185
Outstanding restricted stock units	18,039	50,192
Shares available for further issuance under the 2014 Plan	—	6,255
2024 Equity Incentive Plan:		
Outstanding restricted stock units	4,217	—
Shares available for future issuance under the 2024 Plan	57,591	—
2024 Employee Stock Purchase Plan	4,201	—
Total shares of common stock reserved	93,618	139,215

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, 2022	4,693,880	$ 5.22	5.9	$ 68,795
Granted	178,924	20.87		
Exercised	(669,122)	5.70		9,973
Cancelled	(105,648)	8.18		
Outstanding as of January 31, 2023	4,098,034	$ 5.74	5.0	$ 66,017
Granted	—	—		
Exercised	(884,012)	3.83		17,771
Cancelled	(29,002)	10.40		
Outstanding as of January 31, 2024	3,185,020	$ 6.23	4.2	$ 71,347
Granted	8,000,000	32.00		
Exercised	(1,548,712)	5.50		54,160
Cancelled	(66,174)	18.94		
Outstanding as of January 31, 2025	9,570,134	$ 27.80	8.2	$ 435,133
Vested and exercisable as of January 31, 2025	2,352,521	$ 15.02	5.1	$ 137,044

The weighted-average grant date fair value of options granted to employees was $14.07 for the fiscal year ended January 31, 2023. There were no options with only a service-based vesting condition granted during each of the fiscal years ended January 31, 2025 and 2024.

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.

The assumptions used in the Black-Scholes option pricing model were as follows:

	Year Ended January 31, 2023
Expected term (in years)	6.0 - 6.0
Expected volatility	58.2% - 83.2%
Risk-free interest rate	2.7% - 3.8%
Dividend yield	—

As of January 31, 2025, there was approximately $90.7 million of unrecognized stock-based compensation expense related to stock options, which is expected to be recognized over a weighted-average period of 2.5 years.

CEO Performance Award

In June 2022, the Company's board of directors approved the grant of a stock option under the 2014 Plan to the Company's CEO, Mr. Sinha, to purchase up to 8,000,000 of Class B common stock, contingent and effective upon a listing event, which includes the Company's IPO (the "CEO Performance Award" or "the Award"). The CEO Performance Award was granted upon the Company's IPO in April 2024.

The CEO Performance Award consists of 10 tranches that may be earned as specified in the table below, subject to both 1) a service-based condition and 2) the achievement of Target Stock Value prior to the applicable Option Valuation Expiration Date. Stock price measurement will not commence until the expiration of any lock-up period. Target Stock Value with respect to the Award is based on the percentage of the IPO Price and will be achieved on the date when the volume-weighted average price of the Company's Class A common stock over a period of 90 consecutive days equals or exceeds the applicable Target Stock Value. The exercise price per share of the Award is the IPO Price. Each tranche of the Award will vest on the first date following satisfaction of both the service-based condition and the Target Stock Value subject to Mr. Sinha's continued service with the Company. The shares underlying each tranche will satisfy the service-based condition in 20 equal quarterly installments beginning in January 2022 and will expire in 10 years after the grant date.

Tranche	Target Stock Value	Number of Stock Options Eligible to Vest	Option Valuation Expiration Date
1	$42.88	666,667	Fifth anniversary of the Company's IPO
2	$53.76	666,667	
3	$64.64	666,667	
4	$75.52	666,667	
5	$86.40	666,667	Seventh anniversary of the Company's IPO
6	$96.96	666,667	
7	$107.84	666,667	
8	$118.72	666,667	
9	$161.92	1,333,332	
10	$242.88	1,333,332	

The Company calculated the grant date fair value of the CEO Performance Award based on multiple stock price paths developed through the use of a Monte Carlo simulation model. A Monte Carlo simulation model also calculates a derived service period for each of the 10 vesting tranches, which is the measure of the expected time to achieve each Target Stock value under the scenarios where the Target Stock Value is in fact achieved prior to the Option Valuation Expiration Date. A Monte Carlo simulation model requires the use of various assumptions, including the underlying stock price, volatility, and the risk-free interest rate as of the valuation date, corresponding to the time to expiration of the options, and expected dividend yield. The weighted-average grant date fair value of the CEO Performance Award was $17.37 per share. The Company will recognize total stock-based compensation expense of $139.0 million over the derived service period of each tranche, which is between 1.2 to 4.5 years, using the accelerated attribution method as long as the CEO satisfies the service-based vesting condition. If the Target Stock Value is met sooner than the derived service period, the Company will adjust its stock-based compensation to reflect the cumulative expense associated with the vested awards. Provided that Mr. Sinha continues to be the Company's CEO, the Company will recognize stock-based compensation expense over the requisite service period, regardless of whether the Target Stock Values are achieved.

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 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
Outstanding as of January 31, 2022	31,209,565	$ 11.31
Granted	11,195,973	19.92
Vested	(54,010)	8.48
Forfeited	(2,641,160)	14.75
Outstanding as of January 31, 2023	39,710,368	13.51
Granted	13,443,534	23.78
Vested	(18,000)	28.66
Forfeited	(2,962,232)	17.17
Unvested as of January 31, 2024	50,173,670	16.09
Vested and not yet released	18,000	28.66
Outstanding as of January 31, 2024	50,191,670	16.09
Granted	13,744,702	37.99
Vested	(38,940,299)	15.22
Forfeited	(2,780,324)	23.73
Unvested as of January 31, 2025	22,215,749	31.30
Vested and not yet released	40,625	11.35
Outstanding as of January 31, 2025	22,256,374	$ 31.26

In February 2024, we modified an existing service- performance-, and market-based condition equity award of 1,158,082 RSUs by extending the expiration date from May 2, 2025 to May 2, 2028. The performance-based condition related to the occurrence of a qualifying event was satisfied at the completion of the Company's IPO. The total incremental fair value resulting from the modification was $24.1 million and the total stock-based compensation expense of the equity award of $30.4 million is recorded over the requisite service period. As of January 31, 2025, the Company has recognized all stock-based compensation expense for this equity award.

For the fiscal years ended January 31, 2025, 2024 and 2023, the total grant date fair value of vested RSUs was $592.8 million, $0.5 million and $1.1 million, respectively.

As of January 31, 2025, there was approximately $434.0 million of unrecognized stock-based compensation expense relating to RSUs, which is expected to be recognized over a weighted-average period of 1.9 years.

2024 Employee Stock Purchase Plan

In April 2024, the Company's 2024 ESPP became effective. The 2024 ESPP allows eligible employees to purchase shares of Class A common stock at a discount through payroll deductions of up to 15% of their eligible compensation, subject to any plan limitations. Except for the initial offering period, the 2024 ESPP provides for 24-month offering periods beginning March 21 and September 21 of each year, and each offering period will consist of four six-month purchase periods. The initial offering period began on April 24, 2024, and will end on March 20, 2026.

On each purchase date, eligible employees will purchase Class A common stock at a price per share equal to 85% of the lesser of (1) the fair market value of the Class A common stock on the offering date, or (2) the fair market value of the Class A common stock on the purchase date. For the first offering period, which began on April 24, 2024, the fair market value of the Class A common stock on the offering date was $32.00, the price at which the Company's common stock was first sold to the public in the IPO, as specified in the final prospectus filed with the SEC on April 26, 2024, pursuant to Rule 424(b).

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

	Year Ended January 31, 2025
Expected term (in years)	0.4 - 2.0
Expected volatility	56.5% - 71.7%
Risk-free interest rate	3.6% - 5.4%
Dividend yield	—

As of January 31, 2025, there was approximately $11.4 million of unrecognized stock-based compensation expense related to the ESPP, which is expected to be recognized over a weighted-average period of 0.9 years.

Stock-Based Compensation Expense

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

	Year Ended January 31,		
	2025	2024	2023
Cost of revenue			
Subscription	$ 49,514	$ 45	$ 53
Maintenance	3,076	7	34
Other	14,451	11	140
Research and development	297,051	3,590	3,044
Sales and marketing	330,443	1,313	2,399
General and administrative	219,378	749	1,284
Total stock-based compensation expense	$ 913,913	$ 5,715	$ 6,954

Note 12 – 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):

	Year Ended January 31,					
	2025		2024		2023	
	Class A	Class B	Class A	Class B	Class A	Class B
Numerator:						
Net loss	$ 428,333	$ 726,487	$ —	$ (354,158)	$ —	$ (277,746)
Denominator:						
Weighted-average common stock shares used in computing net loss per share, basic and diluted	57,229	97,065	—	55,228	—	54,190
Weighted-average founders stock shares used in computing net loss per share, basic and diluted	—	—	—	5,400	—	5,400
Net loss per common stock share, basic and diluted	$ 7.48	$ 7.48	$ —	$ (5.84)	$ —	$ (4.66)
Net loss per founders stock share, basic and diluted	$ —	$ —	$ —	$ (5.84)	$ —	$ (4.66)

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):

	Year Ended January 31,		
	2025	2024	2023
Redeemable convertible preferred stock	—	74,183	74,183
Issued and outstanding common stock options	9,570	3,185	4,098
Unvested RSUs issued and outstanding	22,216	50,174	39,710
Total	31,786	127,542	117,991

Note 13 – Income Taxes

U.S. and foreign components of consolidated loss before income taxes were as follows (in thousands):

	Year Ended January 31,		
	2025	2024	2023
Domestic	$ (1,223,181)	$ (356,015)	$ (296,975)
Foreign	74,729	28,546	27,825
Loss before income taxes	$ (1,148,452)	$ (327,469)	$ (269,150)

The provision for income taxes was as follows (in thousands):

	Year Ended January 31,		
	2025	2024	2023
Current:			
Federal	$ (2,330)	$ 2,336	$ —
State	(1,315)	2,818	189
Foreign	8,772	19,598	3,959
Total current provision for income taxes	5,127	24,752	4,148
Deferred:			
Federal	—	—	—
State	—	—	—
Foreign	1,241	1,937	4,448
Total deferred provision for income taxes	1,241	1,937	4,448
Total provision for income taxes	$ 6,368	$ 26,689	$ 8,596

The reconciliation of the statutory federal income tax rate to the Company's effective tax rate is as follows:

	Year Ended January 31,		
	2025	2024	2023
Provision at federal statutory rate	21.0 %	21.0 %	21.0 %
State, net of federal benefit	3.2	—	3.5
Stock-based compensation	10.4	0.3	(0.3)
Impact of foreign operations	2.9	(5.1)	(2.8)
Change in valuation allowance	(42.8)	(14.5)	(27.8)
Research and development credits	4.9	3.9	4.0
Non-deductible expenses	—	(12.8)	—
Other adjustments	(0.2)	(1.0)	(0.8)
Effective income tax rate	(0.6)%	(8.2)%	(3.2)%

Deferred income taxes reflect the net tax effects of temporary differences between the carrying amounts of assets and liabilities for financial reporting purposes and the amounts used for income tax purposes at the enacted rates. The significant components of the Company's deferred tax assets and liabilities were as follows (in thousands):

	January 31,	
	2025	2024
Deferred tax assets:		
Net operating loss carryforwards	$ 330,908	$ 131,449
Capitalized research and development expenditures	208,690	74,843
Research and development credit carryforward	117,837	52,152
Deferred revenue	151,326	119,531
Stock-based compensation	68,587	3,716
Operating lease liabilities	4,863	7,063
Other	26,505	9,578
Total deferred tax assets	908,716	398,332
Less: valuation allowance	(863,039)	(371,027)
Total deferred tax assets, net	45,677	27,305
Deferred tax liabilities:		
State income taxes	(28,936)	(13,493)
Capitalized internal-use software	(5,472)	(3,769)
ROU assets	(4,219)	(6,402)
Other	(18,394)	(13,744)
Total deferred tax liabilities	(57,021)	(37,408)
Net deferred tax assets (liabilities)	$ (11,344)	$ (10,103)

The valuation allowance increased by $492.0 million for the fiscal year ended January 31, 2025. The Company believes that, based on a number of factors, the available objective evidence creates sufficient uncertainty regarding the realizability of the deferred tax assets such that a valuation allowance has been recorded. These factors include the Company's history of net losses since its inception, expected near-term future losses, and the absence of taxable income in prior carryback years. The Company expects to maintain a valuation allowance until circumstances change.

As of January 31, 2025, the Company had U.S. federal net operating loss carryforwards of approximately $1,346.1 million, state net operating loss carryforwards of approximately $626.2 million, and foreign net operating loss carryforwards of approximately $6.0 million. A portion of the U.S. federal net operating loss carryforwards will begin to expire in fiscal 2037. The state net operating loss carryforwards will begin to expire in fiscal 2028. The foreign net operating loss carryforwards do not expire.

As of January 31, 2025, the Company had U.S. federal research and development tax credit carryforwards of approximately $88.0 million, which if not utilized, will begin to expire in fiscal 2036. As of January 31, 2025, the Company had state research and development tax credit carryforwards of approximately $59.3 million. The state credit carryforwards do not expire.

Utilization of the net operating loss and tax credit carryforwards may be subject to an annual limitation due to the "ownership change" limitation provided by Section 382 and 383 of the Internal Revenue Code ("IRC") of 1986, as amended, and other similar state provision. Any future annual limitation may result in the expiration of net operating loss and tax credit carryforwards before utilization.

The following is a tabular reconciliation of the total amounts of unrecognized tax benefits (in thousands):

	January 31,		
	2025	2024	2023
Unrecognized tax benefits at beginning of period	$ 31,263	$ 11,206	$ 7,811
Decreases related to prior year tax positions	(567)	—	—
Increases related to prior year tax positions	—	63	463
Increases related to current year tax positions	15,928	19,994	2,932
Unrecognized tax benefits at end of period	$ 46,624	$ 31,263	$ 11,206

In the fiscal year ended January 31, 2025, the Company recorded an increase in its unrecognized tax benefits related to US federal and California research tax credits. Certain research tax credits have not been utilized on any tax return and currently have no impact on the Company's tax expense due to the Company's operating losses and the related valuation allowances.

The Company's policy is to record interest and penalties related to uncertain tax positions within the provision for income taxes. To date, the combined amounts of accrued interest and penalties included in long-term income taxes payable related to tax positions taken on the Company's tax returns were not material.

The Company files income tax returns with the U.S. federal government and certain state and foreign jurisdictions. The Company's tax returns remain open to examination for the periods ended January 31, 2016 to January 31, 2025.

Note 14 – 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 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.

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

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

	Year Ended January 31,		
	2025	2024	2023
Total revenue	$ 886,544	$ 627,892	$ 599,819
Less:			
Adjusted subscription cost of revenue [1]	161,576	96,053	61,132
Remaining cost of revenue	24,593	40,235	112,567
Remaining research and development expenses	226,235	194,639	163,450
Remaining sales and marketing expenses	531,154	475,687	411,702
Remaining general and administrative expenses	131,462	95,431	82,060
Stock-based compensation expense [2]	913,913	5,715	6,954
Depreciation and amortization	27,970	24,962	22,680
Amortization of acquired intangibles	3,673	1,676	822
Interest expense	41,253	30,295	11,709
Income tax expense	6,368	26,689	8,596
Other items [3]	(1,480)	1,884	1,033
Plus:			
Interest income	25,353	11,216	5,140
Segment net loss	(1,154,820)	(354,158)	(277,746)
Consolidated net loss	$ (1,154,820)	$ (354,158)	$ (277,746)

(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):

	Year Ended January 31,		
	2025	2024	2023
Subscription cost of revenue	$ 215,036	$ 97,927	$ 62,294
Less:			
Stock-based compensation expense	49,514	45	53
Amortization of acquired intangibles	3,673	1,676	822
Stock-based compensation from amortization of capitalized internal-use software	273	153	287
Adjusted subscription cost of revenue	$ 161,576	$ 96,053	$ 61,132

(2) See Note 11 for stock-based compensation expense by captions.

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

The following table presents the Company's long-lived assets, including property and equipment, net and ROU assets, by geographic region (in thousands):

	January 31,	
	2025	2024
United States	$ 62,455	$ 61,402
India	10,453	10,633
Rest of world	6,192	5,671
Total long-lived assets	$ 79,100	$ 77,706

Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosure

None.

Item 9A. 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 Annual Report on Form 10-K. 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 Annual Report on Form 10-K, our disclosure controls and procedures were effective at the reasonable assurance level.

Management's Report on Internal Control over Financial Reporting

This Annual Report on Form 10-K does not include a report of management's assessment regarding internal control over financial reporting or an attestation report of our independent registered public accounting firm due to a transition period established by rules of the SEC for newly public companies.

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 fourth quarter of fiscal year ended January 31, 2025 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.

Item 9B. Other Information

Trading Arrangements

During the quarter ended January 31, 2025, our directors and officers (as defined in Rule 16a-1(f) under the Exchange Act) adopted or terminated the Rule 10b5-1 trading arrangements (as defined in Item 408(a) of Regulation S-K) described below:

On January 15, 2025, 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 April 16, 2026 of up to 150,000 shares of our Class A common stock. The actual number of shares sold will be dependent on the satisfaction of certain conditions set forth in the written plan. Immediately prior to his adoption of the aforementioned trading arrangement, on January 15, 2025, Mr. Choudary terminated a trading arrangement intended to satisfy the affirmative defense conditions of Rule 10b5-1(c) originally adopted on July 15, 2024 for the sales up to 237,600 shares of our Class A common stock. The trading arrangement was originally scheduled to terminate on the earlier of the date all shares under the written plan were sold or October 31, 2025.

Item 9C. Disclosure Regarding Foreign Jurisdictions that Prevent Inspections

Not applicable.

PART III

Item 10. Directors, Executive Officers and Corporate Governance

Code of Conduct

We maintain a Global Code of Conduct that is applicable to all our employees, executive officers and directors. Our Global Code of Conduct is available on our Investor Relations website at ir.rubrik.com under “Governance - Governance Documents”. We intend to satisfy the disclosure requirement under Item 5.05 of Form 8-K regarding amendments to, or waiver from, a provision of our Global Code of Conduct by posting such information on the website address and location specified above. The inclusion of our website address in this Annual Report on Form 10-K does not include or incorporate by reference into this Annual Report on Form 10-K the information on or accessible through our website.

Insider Trading Policy

We have adopted insider trading policies and procedures governing the purchase, sale, and other dispositions of our securities by directors, officers, and employees, and by the Company itself, that are designed to promote compliance with insider trading laws, rules, and regulations, and applicable NYSE listing standards, as well as procedures designed to further the foregoing purposes. A copy of our insider trading policy is filed with this Annual Report on Form 10-K as Exhibit 19.1.

The remaining information required by this item will be set forth under the caption “Proposal 1 Election of Directors”, “Delinquent Section 16(a) Reports”, “Information Regarding the Board and Corporate Governance,” and “Insider Trading Policy” and is incorporated by reference to the definitive Proxy Statement for the 2025 Annual Meeting of Stockholders, which will be filed with the SEC no later than 120 days after January 31, 2025.

Item 11. Executive Compensation

The information required by this item will be set forth under the caption “Executive Compensation” and “Information Regarding the Board and Corporate Governance” and is incorporated by reference to the definitive Proxy Statement for the 2025 Annual Meeting of Stockholders, which will be filed with the SEC no later than 120 days after January 31, 2025.

Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters

The information required by this item will be set forth under the caption “Security Ownership of Certain Beneficial Owners and Management” and “Securities Authorized for Issuance Under Equity Compensation Plans” and is incorporated by reference to the definitive Proxy Statement for the 2025 Annual Meeting of Stockholders, which will be filed with the SEC no later than 120 days after January 31, 2025.

Item 13. Certain Relationships and Related Transactions, and Director Independence

The information required by this item will be set forth under the caption “Transactions with Related Persons and Indemnification” and “Information Regarding the Board and Corporate Governance” and is incorporated by reference to the definitive Proxy Statement for the 2025 Annual Meeting of Stockholders, which will be filed with the SEC no later than 120 days after January 31, 2025.

Item 14. Principal Accountant Fees and Services

The information required by this item will be set forth under the caption “Principal Accountant Fees and Services” and is incorporated by reference to the definitive Proxy Statement for the 2025 Annual Meeting of Stockholders, which will be filed with the SEC no later than 120 days after January 31, 2025.

PART IV

Item 15. Exhibits and Financial Statement Schedules

The following documents are filed as part of this Annual Report on Form 10-K:

a. *Consolidated Financial Statements*

The consolidated financial statements are filed as part of this Annual Report on Form 10-K under "Item 8. Financial Statements and Supplementary Data."

b. *Financial Statement Schedules*

The financial statement schedules are omitted because they are either not applicable or the information required is presented in the financial statements and notes thereto under "Item 8. Financial Statements and Supplementary Data."

c. *Exhibits*

The exhibits listed in the following Exhibit Index are filed, furnished, or incorporated by reference as part of this Annual Report on Form 10-K.

Exhibit Index

		Incorporated by Reference				
Exhibit Number	**Description of Exhibit**	**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	
4.1	Form of Class A Common Stock Certificate of the Registrant	S-1/A	333-278434	4.1	4/16/2024	
4.2	Description of Securities					X
4.3	Amended and Restated Investors' Rights Agreement, by and among the Registrant and certain of its stockholders, dated December 7, 2018.	S-1	333-278434	4.2	4/1/2024	
10.1+	2024 Equity Incentive Plan.	S-1/A	333-278434	10.3	4/16/2024	
10.2+	Forms of Stock Option Grant Notice, Stock Option Agreement, and Notice of Exercise, Restricted Stock Award Agreement, and Restricted Stock Unit Award Agreement under the 2024 Stock Option and Grant Plan.	S-1/A	333-278434	10.4	4/16/2024	
10.3+	2024 Employee Stock Purchase Plan.	S-1/A	333-278434	10.5	4/16/2024	
10.4+	Amended and Restated 2014 Stock Option and Grant Plan.	S-1	333-278434	10.1	4/1/2024	
10.5+	Forms of Stock Option Grant Notice, Stock Option Agreement, and Notice of Exercise, Restricted Stock Award Agreement, and Restricted Stock Unit Award Agreement under the Amended and Restated 2014 Stock Option and Grant Plan.	S-1	333-278434	10.2	4/1/2024	
10.6+	Non-Employee Director Compensation Policy.	S-1	333-278434	10.6	4/1/2024	
10.7+	Severance and Change in Control Plan.	S-1	333-278434	10.7	4/1/2024	
10.8+	Form of Indemnity Agreement entered into by and between Rubrik, Inc. and each director and executive officer.	S-1	333-278434	10.8	4/1/2024	
10.9+	Confirmatory Offer Letter, dated September 5, 2023, by and between the Company and Bipul Sinha.	S-1	333-278434	10.9	4/1/2024	
10.10+	Confirmatory Offer Letter, dated September 5, 2023, by and between the Company and Kiran Choudary.	S-1	333-278434	10.10	4/1/2024	
10.11+	Confirmatory Offer Letter, dated September 5, 2023, by and between the Company and Arvind Nithrakashyap.	S-1	333-278434	10.11	4/1/2024	
10.12+	Confirmatory Offer Letter, dated September 5, 2023, by and between the Company and Brian McCarthy.	S-1	333-278434	10.12	4/1/2024	
10.13	Sublease, dated September 24, 2018, by and between the Company and Pivotal Software, Inc.	S-1	333-278434	10.13	4/1/2024	
10.14	First Amendment to Sublease, dated December 4, 2020, by and between the Registrant and Pivotal Software, Inc.	S-1	333-278434	10.14	4/1/2024	
10.15	Amended and Restated Credit Agreement, dated August 17, 2023, by and between the Registrant and Goldman Sachs BDC, Inc.	S-1	333-278434	10.15	4/1/2024	

10.16†	Original Equipment Manufacturer (OEM) Purchase Agreement, dated November 19, 2020, by and between the Registrant and Super Micro Computer, Inc.	S-1	333-278434	10.16	4/1/2024	
10.17†	Distribution Addendum to the OEM Purchase Agreement, dated May 27, 2022, by and between the Registrant and Super Micro Computer, Inc.	S-1	333-278434	10.17	4/1/2024	
19.1	Insider Trading Policy					X
21.1	List of subsidiaries					X
23.1	Consent of KPMG LLP, independent registered public accounting firm					X
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
97.1	Incentive Compensation Recoupment Policy					X
101	The following financial information from Rubrik Inc.'s Annual Report on Form 10-K for the fiscal year ended January 31, 2025 formatted in Inline XBRL (Extensible Business Reporting Language) includes: (i) the Consolidated Balance Sheets, (ii) the Consolidated Statements of Operations, (iii) the Consolidated Statements of Comprehensive Loss, (iv) the Consolidated Statements of Redeemable Convertible Preferred Stock and Stockholders' Deficit, (v) the Consolidated Statements of Cash Flows, and (vi) Notes to the Consolidated Financial Statements.					X
104	Cover Page Interactive Data File (formatted as inline XBRL and contained in Exhibits 101).					X

+ Indicates management contract or compensatory plan.

† Certain portions of this exhibit (indicated by asterisks) have been omitted because they are both not material and are the type that the Company treats as private or confidential.

* The certifications furnished in Exhibits 32.1 and 32.2 hereto are deemed to accompany this Annual Report on Form 10-K 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.

Item 16. Form 10–K Summary

None.

SIGNATURES

Pursuant to the requirements of Section 13 or 15(d) 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: March 20, 2025

Rubrik, Inc.

By: /s/ Bipul Sinha

Name: Bipul Sinha

Title: Chief Executive Officer
(Principal Executive Officer)

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed below by the following persons on behalf of the registrant and in the capacities and on the dates indicated.

Signature	Title	Date
/s/ Bipul Sinha Bipul Sinha	Chief Executive Officer and Director (Principal Executive Officer)	March 20, 2025
/s/ Kiran Choudary Kiran Choudary	Chief Financial Officer (Principal Financial Officer and Principal Accounting Officer)	March 20, 2025
/s/ Asheem Chandna Asheem Chandna	Director	March 20, 2025
/s/ R. Scott Herren R. Scott Herren	Director	March 20, 2025
/s/ Mark D. McLaughlin Mark D. McLaughlin	Director	March 20, 2025
/s/ Ravi Mhatre Ravi Mhatre	Director	March 20, 2025
/s/ Arvind Nithrakashyap Arvind Nithrakashyap	Chief Technology Officer and Director	March 20, 2025
/s/ Enrique Salem Enrique Salem	Director	March 20, 2025
/s/ John W. Thompson John W. Thompson	Director	March 20, 2025
/s/ Yvonne Wassenaar Yvonne Wassenaar	Director	March 20, 2025

DESCRIPTION OF THE REGISTRANT'S SECURITIES REGISTERED PURSUANT TO SECTION 12 OF THE SECURITIES EXCHANGE ACT OF 1934

The following is a summary of the rights of our common and preferred stock and some of the provisions of our amended and restated certificate of incorporation, amended and restated bylaws, investors' rights agreement, and relevant provisions of Delaware General Corporation Law. The descriptions herein are qualified in their entirety by our amended and restated certificate of incorporation, amended and restated bylaws, and investors' rights agreement, copies of which have been filed as exhibits to our Annual Report on Form 10-K, as well as the relevant provisions of Delaware General Corporation Law.

General

Our amended and restated certificate of incorporation provides for two classes of common stock: Class A common stock and Class B common stock, and it authorizes shares of undesignated preferred stock, the rights, preferences and privileges of which may be designated from time to time by our board of directors.

Our authorized capital stock consists of the following shares, all with a par value of $ 0.000025 per share, of which:

- 1,070,000,000 shares are designated as Class A common stock;
- 210,000,000 shares are designated as Class B common stock; and
- 20,000,000 shares are designated as preferred stock.

Class A and Class B Common Stock

Voting Rights

Holders of our Class A common stock are entitled to one vote per share on any matter that is submitted to a vote of our stockholders. Holders of our Class B common stock are entitled to 20 votes per share on any matter submitted to our stockholders. The holders of our Class A common stock and Class B common stock will vote together as a single class on all matters (including the election of directors) submitted to a vote of stockholders, unless otherwise required by Delaware law.

Under Delaware law, holders of our Class A common stock or Class B common stock would be entitled to vote as a separate class if a proposed amendment to our amended and restated certificate of incorporation would increase or decrease the aggregate number of authorized shares of such class, increase or decrease the par value of the shares of such class, or alter or change the powers, preferences, or special rights of the shares of such class so as to affect them adversely. As a result, in these limited instances, the holders of a majority of the Class A common stock could defeat any amendment to our amended and restated certificate of incorporation. For example, if a proposed amendment of our amended and restated certificate of incorporation provided for the Class A common stock to rank junior to the Class B common stock with respect to (1) any dividend or distribution, (2) the distribution of proceeds were we to be acquired, or (3) any other right, Delaware law would require the vote of the Class A common stock. In this instance, the holders of a majority of Class A common stock could defeat that amendment to our amended and restated certificate of incorporation.

Our amended and restated certificate of incorporation does not provide for cumulative voting for the election of directors.

Economic Rights

Except as expressly provided in our amended and restated certificate of incorporation or required by applicable law, all shares of Class A common stock and Class B common stock have the same rights and privileges and rank equally, share ratably, and are identical in all respects for all matters, including those described below.

Dividends and Distributions

Subject to preferences that may apply to any shares of preferred stock outstanding at the time, the holders of Class A common stock and Class B common stock will be entitled to share equally, identically, and ratably, on a per share basis, with respect to any dividend or distribution of cash or property paid or distributed by the company, unless different treatment of the shares of the affected class is approved by the affirmative vote of the holders of a majority of the outstanding shares of such affected class, voting separately as a class.

Under Delaware law, we can only pay dividends either out of "surplus" or out of the current or the immediately preceding fiscal year's net profits. Surplus is defined as the excess, if any, at any given time, of the total assets of a corporation over its total liabilities and statutory capital. The value of a corporation's assets can be measured in a number of ways and may not necessarily equal their book value.

Right to Receive Liquidation Distributions

On our liquidation, dissolution, or winding-up, the holders of Class A common stock and Class B common stock will be entitled to share equally, identically, and ratably in all assets remaining after the payment of any liabilities, liquidation preferences, and accrued or declared but unpaid dividends, if any, with respect to any outstanding preferred stock, unless a different treatment is approved by the affirmative vote of the holders of a majority of the outstanding shares of such affected class, voting separately as a class.

Change of Control Transactions

The holders of Class A common stock and Class B common stock will be treated equally and identically with respect to shares of Class A common stock or Class B common stock owned by them, unless different treatment of the shares of each class is approved by the affirmative vote of the holders of a majority of the outstanding shares of the class treated differently, voting separately as a class, on (a) the closing of the sale, transfer, or other disposition of all or substantially all of our assets, (b) the consummation of a consolidation, merger, or reorganization which results in our voting securities outstanding immediately before the transaction (or the voting securities issued with respect to our voting securities outstanding immediately before the transaction) representing less than a majority of the combined voting power of the voting securities of the company or the surviving or acquiring entity, or (c)

the closing of the transfer (whether by merger, consolidation, or otherwise), in one any transaction or a series of related transactions, to a person or group of affiliated persons of securities of the company if, after closing, the transferee person or group would hold 50% or more of the company's outstanding voting power of the company (or the surviving or acquiring entity). However, consideration to be paid or received by a holder of common stock in connection with any such assets sale, consolidation, merger, or reorganization under any employment, consulting, severance, or other compensatory arrangement will be disregarded for the purposes of determining whether holders of common stock are treated equally and identically.

Subdivisions and Combinations

If we subdivide or combine in any manner outstanding shares of Class A common stock or Class B common stock, the outstanding shares of the other class will be subdivided or combined in the same proportion and manner.

No Preemptive or Similar Rights

Our Class A common stock and Class B common stock are not entitled to preemptive rights, and are not subject to conversion, redemption, or sinking fund provisions, except for the conversion provisions with respect to the Class B common stock described below.

Conversion

Each outstanding share of Class B common stock is convertible at any time at the option of the holder into one share of Class A common stock. In addition, each share of Class B common stock will convert automatically into one share of Class A common stock upon any transfer, whether or not for value, except for certain permitted transfers set forth in our amended and restated certificate of incorporation, including, but not limited to, transfers to certain trusts for estate planning purposes and entities under common control with or controlled by such holder of our Class B common stock.

All of the outstanding shares of Class B common stock will convert automatically into shares of Class A common stock upon the earliest to occur of: (i) the date fixed by our board of directors that is no less than 61 days and no more than 180 days following the date on which the outstanding shares of Class B common stock represent less than 5% of the then outstanding shares of Class A and Class B common stock; (ii) April 29, 2034; (iii) the date fixed by our board of directors that is no less than 61 days and no more than 180 days following the date on which our co-founder Bipul Sinha is no longer providing services to Rubrik as an officer, employee, or director; (iv) the date fixed by our board of directors that is no less than 61 days and no more than 180 days following the death or incapacity of Mr. Sinha; or (v) the date specified by a vote of the holders of a majority of the outstanding shares of Class B common stock.

Once converted into Class A common stock, the Class B common stock will not be reissued.

Preferred Stock

Our board of directors may, without further action by our stockholders, fix the rights, preferences, privileges, and restrictions of up to an aggregate of 20,000,000 shares of preferred stock in one or more series and authorize their issuance. These rights, preferences, and privileges could include dividend rights, conversion rights, voting rights, terms of redemption, liquidation preferences, sinking fund terms, and the number of shares constituting any series or the designation of such series, any or all of which may be greater than the rights of our common stock. The issuance of our preferred stock could adversely affect the voting power of holders of our common stock, and the likelihood that such holders will receive dividend payments and payments upon liquidation. In addition, the issuance of preferred stock could have the effect of delaying, deferring, or preventing a change of control or other corporate action.

Registration Rights

We are party to an investors' rights agreement that provides that certain holders of our common stock have certain registration rights as set forth below. The registration of shares of our common stock by the exercise of registration rights described below would enable the holders to sell these shares without restriction under the Securities Act when the applicable registration statement is declared effective. We will pay the registration expenses, other than underwriting discounts and commissions, of the shares registered by the demand, piggyback, and Form S-3 registrations described below.

Generally, in an underwritten offering, the managing underwriter, if any, has the right, subject to specified conditions, to limit the number of shares such holders may include. The demand, piggyback, and Form S-3 registration rights described below will expire after the earlier of April 29, 2029, or with respect to any particular stockholder, such time that such stockholder can sell all of its shares entitled to registration rights under Rule 144 of the Securities Act during any 90-day period.

Demand Registration Rights

Certain holders of our common stock are entitled to certain demand registration rights. These holders may request that we register all or a portion of the registrable shares. We are obligated to effect only two such registration. Such request for registration must cover at least that number of registrable shares as would have an anticipated aggregate offering price of at least $15.0 million.

Piggyback Registration Rights

Certain holders of our common stock are entitled to certain piggyback registration rights. If we register any securities for public sale, either for our own account or for the account of other security holders, we will also have to register all registrable securities that the holders of such securities request in writing to be registered. This piggyback registration right does not apply to (i) a registration relating to the demand registration rights set forth above, (ii) a registration relating solely to the issuance of securities by us or a subsidiary pursuant to a stock option, stock purchase, or similar plan, (iii) a registration relating to a corporate reorganization or transaction under Rule 145 of the Securities Act, (iv) a registration on any form that does not include substantially the same information as would be required to be included in a registration statement covering the sale of the shares held by the holders, or (v) a registration in which the only common stock being registered is common stock issued upon conversion of debt securities that are also being registered, the holders of these shares are entitled to notice of the registration, and have the right to include their shares in the registration, subject to limitations that the underwriters may impose on the number of shares included in the offering.

Form S-3 Registration Rights

Certain holders of our common stock are entitled to certain registration rights on Form S-3. The holders of these shares can make a request that we register their shares on Form S-3 if we are qualified to file a registration statement on Form S-3 and if the anticipated aggregate price of the shares would be at least $1.0 million. We are not required to effect more than two Form S-3 registration statements within any 12-month period.

Anti-Takeover Effects of Delaware Law and Our Certificate of Incorporation and Bylaws

Some provisions of Delaware law, our amended and restated certificate of incorporation, and our amended and restated bylaws contain provisions that could make the following transactions more difficult: an acquisition of us by means of a tender offer, a proxy contest or otherwise; or the removal of our incumbent officers and directors. It is possible that these provisions could make it more difficult to accomplish or could deter transactions that stockholders may otherwise consider to be in their best interest or in our best interests, including transactions which provide for payment of a premium over the market price for our shares.

These provisions, summarized below, are intended to discourage coercive takeover practices and inadequate takeover bids. These provisions are also designed to encourage persons seeking to acquire control of us to first negotiate with our board of directors. We believe that the benefits of the increased protection of our potential ability to negotiate with the proponent of an unfriendly or unsolicited proposal to acquire or restructure us outweigh the disadvantages of discouraging these proposals because negotiation of these proposals could result in an improvement of their terms.

Preferred Stock

Our board of directors has the authority, without further action by our stockholders, to issue up to 20,000,000 shares of undesignated preferred stock with rights and preferences, including voting rights, designated from time to time by our board of directors. The existence of authorized but unissued shares of preferred stock would enable our board of directors to render more difficult or to discourage an attempt to obtain control of us by means of a merger, tender offer, proxy contest, or other means.

Stockholder Meetings

Our amended and restated bylaws provide that a special meeting of stockholders may be called only by our chairperson, chief executive officer, or by a resolution adopted by our board of directors.

Requirements for Advance Notification of Stockholder Nominations and Proposals

Our amended and restated bylaws establish advance notice procedures with respect to stockholder proposals to be brought before a stockholder meeting and the nomination of candidates for election as directors, other than nominations made by or at the direction of the board of directors or a committee of the board of directors.

Elimination of Stockholder Action by Written Consent

Our amended and restated certificate of incorporation and amended and restated bylaws eliminate the right of stockholders to act by written consent without a meeting.

Staggered Board

Our board of directors is divided into three classes. The directors in each class serve for a three-year term, one class being elected each year by our stockholders by a plurality of the votes cast. This system of electing and removing directors may tend to discourage a third-party from making a tender offer or otherwise attempting to obtain control of us, because it generally makes it more difficult for stockholders to replace a majority of the directors.

Removal of Directors

Our amended and restated certificate of incorporation provides that no member of our board of directors may be removed from office by our stockholders except for cause and, in addition to any other vote required by law, upon the approval of at least 66 2/3% of the total voting power of all of our outstanding voting stock then entitled to vote in the election of directors.

Stockholders Not Entitled to Cumulative Voting

Our amended and restated certificate of incorporation does not permit stockholders to cumulate their votes in the election of directors.

Delaware Anti-Takeover Statute

We are subject to Section 203 of the Delaware General Corporation Law, which prohibits persons deemed to be "interested stockholders" from engaging in a "business combination" with a publicly held Delaware corporation for three years following the date these persons become interested stockholders unless the business combination is, or the transaction in which the person became an interested stockholder was, approved in a prescribed manner or another prescribed exception applies. Generally, an "interested stockholder" is a person who, together with affiliates and associates, owns, or within three years prior to the determination of interested stockholder status did own, 15% or more of a corporation's voting stock. Generally, a "business combination" includes a merger, asset or stock sale, or other transaction resulting in a financial benefit to the interested stockholder. The existence of this provision may have an anti-takeover effect with respect to transactions not approved in advance by the board of directors.

Choice of Forum

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: (1) any derivative action or proceeding brought on our behalf; (2) any action or proceeding asserting a breach of fiduciary duty; (3) any action or proceeding asserting a claim against us under the Delaware General Corporation Law; (4) any action or proceeding regarding our amended and restated certificate of incorporation or our amended and restated bylaws; (5) any action or proceeding as to which the Delaware General Corporation Law confers jurisdiction to the Court of Chancery of the State of Delaware; or (6) any action or proceeding asserting a claim against us that is governed by the internal affairs doctrine.

This choice of forum provision would not apply to claims brought to enforce a duty or liability created by the Securities Act, the Exchange Act or any other claim for which the federal courts have exclusive jurisdiction. Our amended and restated certificate of incorporation further 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 will be the exclusive forum for resolving any complaint asserting a cause or causes of action arising under the Securities Act, including all causes of action asserted against any defendant to such complaint. In addition, our amended and restated certificate of incorporation 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.

Amendment of Charter Provisions

The amendment of any of the above provisions, except for the provision making it possible for our board of directors to issue preferred stock, would require approval by holders of at least 66 2/3% of the total voting power of all of our outstanding voting stock. The provisions of Delaware law, our amended and restated certificate of incorporation, and our amended and restated bylaws could have the effect of discouraging others from attempting hostile takeovers and, as a consequence, they may also inhibit temporary fluctuations in the market price of our Class A common stock that often result from actual or rumored hostile takeover attempts. These provisions may also have the effect of preventing changes in the composition of our board and management. It is possible that these provisions could make it more difficult to accomplish transactions that stockholders may otherwise deem to be in their best interests.

Transfer Agent and Registrar

The transfer agent and registrar for our Class A common stock and Class B common stock is Equiniti Trust Company, LLC. The transfer agent and registrar's address is 48 Wall Street, Floor 23, New York, NY 10005.

Exchange Listing

Our Class A common stock is listed on the New York Stock Exchange under the symbol "RBRK."

Exhibit 19.1

RUBRIK, INC.

INSIDER TRADING POLICY

(Last amended: March 18, 2025)

The Board of Directors (the "***Board***") of Rubrik, Inc., a Delaware corporation (the "***Company***"), has adopted this Insider Trading Policy (this "***Policy***") to take an active role in the prevention of insider trading violations by the Company's officers, directors, employees, and other related individuals. In addition, it is the Company's policy to comply with applicable laws and regulations related to insider trading when engaging in transactions in the Company's securities.

1. Policy Overview

On a regular basis, the Company provides you, its officers, directors, employees and other related individuals, with confidential information regarding many aspects of its business. Under federal and state securities laws, it is illegal to trade in the securities of a company while in possession of material nonpublic information about that company. Thus, because you will have knowledge of specific confidential information that is not disclosed outside of the Company and which will constitute material nonpublic information, your trading in the Company's securities could constitute "insider trading" and violate the law, as could "tipping" (*i.e.*, giving material nonpublic information to others who then trade on the basis of that information). The consequences of insider trading or the tipping of material nonpublic information can be severe. In fact, the person violating the laws, as well as the Company and its individual directors, officers, and other supervisory personnel, may be subject to criminal and civil lawsuits and financial penalties in connection with a violation of the insider trading laws.

Nonpublic information about the Company is subject to your Confidential Information and Invention Assignment Agreement with the Company and is not to be used or disclosed outside of the Company, except as necessary to perform your job duties. Unauthorized disclosure or use of nonpublic information, including misuse in securities trading, will subject you to disciplinary action, up to and including termination of employment. The Company has adopted this Policy to comply with the laws governing (i) trading in its common stock while in possession of material nonpublic information concerning the Company and (ii) tipping or disclosing material nonpublic information to outsiders, as well as to prevent the appearance of improper trading or tipping. The Company reserves the right to prohibit any transaction from being completed to enforce compliance with this Policy.

In addition, it is the policy of the Company that no person subject to this policy who, in the course of such person's relationship with the Company, learns of any confidential information that is material to another publicly traded company may trade in that other company's securities until the information becomes public or is no longer material to that other company. Moreover, in the course of your relationship with the Company, you may obtain confidential information that is material to one company that could affect the share price of a

different publicly traded company. In such case, you may not trade in the securities of such different publicly traded company until such information becomes public or is no longer material.

2. Components of the Insider Trading Policy

(a) Do not trade on material nonpublic information

Whether or not the trading window (as described below) is open and except as discussed in the section titled "*Exceptions to the Insider Trading Policy*" below, you may not, directly or indirectly through others, engage in any transaction involving the Company's securities *while you are aware of* material nonpublic information about the Company. It is not an excuse that you did not "use" the information in deciding whether or not to engage in the transaction.

Similarly, you may not engage in transactions involving the securities of any other company if you are aware of material nonpublic information either about that company or that could impact the share price of that company. For example, you may be involved in a proposed transaction involving a prospective business relationship or transaction with another company. If information about that transaction constitutes material nonpublic information for that other company, you are prohibited from engaging in transactions involving the securities of that other company. It is important to note that "materiality" is different for different companies. Information that is not material to the Company may be material to another company.

(b) Do not disclose material nonpublic information

You may not disclose material nonpublic information concerning the Company or any other company to friends, family members or any other person or entity not authorized to receive such information, except directly to the Securities and Exchange Commission (the "***SEC***") in compliance with the Company's Whistleblower Policy. Any nonpublic information you acquire in the course of your service with the Company may only be used for legitimate business purposes of the Company. In addition, you are required to handle the nonpublic information of others in accordance with the terms of any relevant nondisclosure agreements, including your employment agreement and/or your Confidential Information and Invention Assignment Agreement with the Company, and to limit your use of the nonpublic information to the purpose for which it was disclosed.

Even if you are not directly disclosing material nonpublic information, you may not make recommendations or express opinions about securities of another company, the Company or otherwise, based on material nonpublic information. In particular, you may not participate, in any manner other than passive observation, in any Internet "chat" room, message board or social media platform that is related to trading in the Company's securities. You are prohibited from engaging in these actions whether or not you derive any profit or personal benefit from doing so. You should know that third parties are known to contact employees of companies to obtain information about the company under false pretexts.

(c) Do not respond to outside inquiries for information

In the event you receive an inquiry for information from someone outside of the Company, you should refer the inquiry to the Company's Chief Legal Officer or, if the Chief Legal Officer is unavailable, the Company's Chief Financial Officer (each, a "***Compliance Officer***"). If you receive an inquiry from a stock analyst or other person from the analyst research community, you should refer the inquiry to the Company's Head of Investor Relations. Responding to a request yourself is a violation of this Policy and, in some circumstances, may be a violation of the law.

(d) Take personal responsibility

The ultimate responsibility for complying with this Policy and applicable laws rests with you. As the Company requests you do in all aspects of your work, please use your best judgment at all times and consult with a Compliance Officer and/or your legal and financial advisors, in confidence, if you have questions.

3. Scope of the Insider Trading Policy – Personnel

This Policy applies to all the Company directors, officers, employees and agents (such as consultants and contractors) and its subsidiaries upon the commencement of their relationship with the Company or any of its subsidiaries.

References in this Policy to "***you***" (as well as general references to the Company directors, officers, employees and agents) should also be understood to include, to the extent applicable, members of your family who reside with you, any other persons with whom you share a household, any family members who do not live in your household but whose transactions in the Company's securities are directed by you or are subject to your influence or control, and any other individuals or entities whose transactions in securities you influence, direct or control (including, for example, a venture or investment fund, if you influence, direct or control transactions by the fund); provided, however, that this Policy does not apply to any such entity that engages in the investment of securities in the ordinary course of its business (e.g., an investment fund or partnership) if such entity has established its own insider trading controls and procedures in compliance with applicable securities laws. The foregoing persons who are deemed subject to this policy are referred to in this policy as "***Related Persons***." You are responsible for making sure that your Related Persons comply with this Policy.

You are expected to comply with this Policy as long as you hold the Company's securities or possess any material nonpublic information about the Company or another applicable publicly traded company as more specifically set forth in this policy. This means that, even after you cease to be affiliated with the Company, you must continue to abide by the applicable trading restrictions until you no longer have material nonpublic information. *In addition, if you are subject to a trading blackout under this Policy at the time you cease to be affiliated with the Company, you are expected to abide by the applicable trading restrictions until at least the end of the relevant blackout period.*

4. Scope of the Insider Trading Policy – Transactions

This Policy applies to all transactions involving the Company's securities, including gifts involving the Company's common stock or transfers for tax planning purposes in which the beneficial ownership and pecuniary interest in the transferred securities does not change. This Policy therefore applies to purchases, sales, gifts and other transfers of the Company's common stock, options, restricted stock units, warrants, debt securities and other securities (including distributions of securities by a venture or other investment fund to its constituent equity holders). Although there are limited exceptions to this Policy (described in "*Exceptions to the Insider Trading Policy*" below), please note that there are no exceptions to insider trading laws or this Policy based on the size of the transaction (*i.e.*, this policy applies whether a trade involves one or 10,000 shares of the Company's common stock).

(a) Transactions that are Strictly Prohibited or Require Special Consideration

(i) Short Sales. You may not engage in short sales (i.e., the sale of a security that must be borrowed to make delivery) or "sell short against the box" (i.e., sell with a delayed delivery) if such sales involve the Company's securities. Short sales may signal to the market possible bad news about the Company or a general lack of confidence in its prospects and an expectation that the value of its securities will decline.

(ii) Derivative or Hedging Transactions. You may not engage in derivative securities or hedging transactions, including prepaid variable forward contracts, equity swaps, collars, and exchange funds, or otherwise engage in transactions that hedge or offset, or are designed to hedge or offset, any decrease in the market value of the Company's securities and the risks associated with holding its common stock. You may not trade in publicly-traded options, such as puts and calls, and other derivative securities with respect to the Company's securities (other than stock options and other compensatory equity awards issued to you by the Company).

(iii) Collateral. You may not use the Company's securities as collateral for loans. You may not pledge the Company's securities as collateral for loans. If you have previously pledged or collateralized your securities of the Company and do not unwind this pledge or collateral position by the end of the second full fiscal quarter following the Company's initial public offering, you must contact the Chief Legal Officer.

(iv) Margin Accounts. You may not hold the Company's common stock in margin accounts because your broker may sell securities held in the margin account during a blackout period.

(v) Pledge. You may not pledge or otherwise use the Company's securities as collateral for a loan unless permitted pursuant to the Company's Pledging Policy and in accordance with the pre-clearance review and approval process required thereby. For the avoidance of doubt, if you have pledged the Company's securities as collateral for a loan as permitted pursuant to the Company's Pledging Policy and in accordance with the pre-clearance review and approval process required thereby, any sale of such securities by the pledgee will not be deemed a transaction under this Policy.

(vi) Standing and Limit Orders. Standing and limit orders (except standing and limit orders under approved trading plans) create heightened risks for insider trading violations similar to the use of margin accounts. There is no control over the timing of purchases or sales that result from standing instructions to a broker, and as a result the broker could execute a transaction when an insider is in possession of material nonpublic information. We therefore

discourage placing standing or limit orders on the Company's securities. You should exercise caution when placing open orders, such as limit orders or stop orders, with brokers, particularly where the order is likely to remain outstanding for an extended period of time. Open orders may result in the execution of a trade during a blackout period, which may result in inadvertent insider trading in violation of this Policy.

5. Definition of "Material Nonpublic Information"

Information is "material" if a reasonable investor would consider it important in making a decision to buy, sell or retain the Company's common stock. Both positive and negative information may be material.

Information is "nonpublic" until it has been widely disseminated to the public (through, for example, an SEC filing, press conference or press release), and the public has had a chance to absorb and evaluate it. Generally speaking, information will be considered publicly disseminated for purposes of this policy at the start of the regular trading session following one full trading day after public announcement. Even after information has been publicly shared, you must wait until the opening of trading on the second full trading day after public disclosure before you can treat it as public. For example, if we announce material information through a press release after trading ends on Wednesday, the material information will not be considered public for purposes of insider trading until the opening of trading on Friday. Depending on the particular circumstances, we may determine that a longer waiting period should apply to the release of specific material nonpublic information.

Unfortunately, there is no bright-line rule on what would qualify as material nonpublic information; rather, materiality is based on an assessment of all of the facts and circumstances, and is often evaluated by relevant enforcement authorities with the benefit of hindsight. The following types of information are some examples of what could be considered material nonpublic information until publicly disclosed. Please note that this list is not exhaustive; there may be other types of information that would qualify as material information as well:

- financial results, financial condition, projections, key metrics, or forecasts;
- known or anticipated, but unannounced, earnings or losses;
- plans to launch new products or features or other significant market initiatives;
- the status of our progress toward achieving significant business or financial goals;
- significant developments involving business relationships with vendors, resellers or other current or prospective partners, including gain or loss of contracts;
- significant corporate events, such as a pending or proposed acquisition;
- public or private sales of our debt or equity securities;
- stock splits, dividends, or changes in dividend policy;
- the establishment of a repurchase program for our securities;
- major contract awards or cancellations;
- significant employee layoffs;
- a disruption in our operations or cybersecurity or other breach or unauthorized access of our property or assets, including our facilities and information technology infrastructure;
- tender offers or proxy fights;
- significant accounting restatements or write-offs;

- significant litigation or settlements, including positive or negative developments;
- impending bankruptcy;
- major product announcements and/or partnerships; or
- known but unannounced changes in our senior management or board of directors.

Financial information is particularly sensitive. For example, nonpublic information about the results of the Company's operations for even a portion of a quarter might be material in helping an analyst predict the Company's results of operations for the quarter.

Information is "nonpublic" until it has been widely disseminated to the public market and the public has had a chance to absorb and evaluate it. Unless you have seen material information publicly disseminated, you should assume the information is nonpublic.

When in doubt, you should assume that the information is both material and nonpublic. If you have any questions as to whether information should be considered material or nonpublic, please consult with a Compliance Officer.

6. When You May Trade in the Company's Common Stock

Even if you are not in possession of any material nonpublic information, you may only trade in the Company's common stock as follows:

(i) Open Trading Window. If you are an officer, director, employee, or other related individual of the Company, you may only engage in transactions involving the Company's common stock during an open trading window. The Company's trading window will typically open at the start of the second full trading day following the date that its quarterly financial results are publicly disclosed and continue through the end of the 15th calendar day of the 3rd month of the quarter. In addition to regular quarterly blackout periods, there may be additional blackout periods when appropriate due to certain events. the Company will notify you whenever a special blackout period goes into effect that applies to you. See "*Company's Blackout Periods*" below.

Pre-Clearance. In addition, if you are a member of the Board or an executive officer of the Company, you must receive pre-clearance from a Compliance Officer for any proposed transaction by you or your Related Persons. This includes even proposed gifts involving the Company's common stock or transfers for tax planning purposes in which the beneficial ownership and pecuniary interest in the transferred securities do not change. From time to time, a Compliance Officer may identify other persons who require pre-clearance on Schedule I hereto. A Compliance Officer may not engage in a transaction involving the Company's common stock unless the other Compliance Officer has pre-cleared the transaction. The Compliance Officer is under no obligation to approve a transaction submitted for pre-clearance and may determine not to permit the transaction.

Please see the section titled "10b5-1 Plans" for information on trading under or entering into a 10b5-1 trading plan.

If you do not follow the above requirements, you may be subject to disciplinary action, up to and including termination of your relationship with the Company, as well as civil and criminal penalties as described in the section titled "*Consequences of Insider Trading*" below.

7. Company's Blackout Periods

To limit the likelihood of trading at times when there is a significant risk of insider trading exposure, the Company has instituted quarterly trading blackout periods and may institute special trading blackout periods from time to time. Whether or not a blackout period is in effect, you must comply with this Policy and may not trade on the basis of material nonpublic information.

(a) Quarterly Blackout Periods

Except as discussed in the section titled "*Exceptions to the Insider Trading Policy*", directors, officers, employees and agents may not engage in transactions involving the Company's common stock during quarterly blackout periods. Quarterly blackout periods begin at the end of the 15th calendar day of the 3rd month of each fiscal quarter and end at the start of the second full trading day following the date of public disclosure of the financial results for that fiscal quarter. This defined period is a particularly sensitive time for transactions involving the Company's common stock from the perspective of compliance with applicable securities laws due to the fact that, during this period, individuals may often possess or have access to material nonpublic information relevant to the expected financial results for the quarter.

Please note that a quarterly blackout period may commence early or may be extended if, in the judgment of the Compliance Officer, there exists undisclosed information that would make trades by persons subject to the quarterly blackout period inappropriate. It is important to note that the fact that a quarterly blackout period has commenced early or has been extended should be considered material nonpublic information that should not be communicated to any other person.

(b) Special Blackout Periods

From time to time, the Company may also implement additional blackout periods when, in the judgment of a Compliance Officer, a trading blackout is warranted. The Company will generally impose special blackout periods when there are material developments known to us that have not yet been disclosed to the public. For example, the Company may impose a special blackout period in anticipation of announcing interim earnings guidance or a significant transaction or business development. However, special blackout periods may be declared for any reason.

The Company will notify you if you are subject to a special blackout period. If you receive this notification, you may not disclose to others the fact that you are subject to the special blackout period and may not engage in any transaction involving the Company's common stock until approved by the Compliance Officer.

(c) Regulation BTR Blackouts

Directors and executives may also be subject to trading blackouts pursuant to Regulation Blackout Trading Restriction ("***Regulation BTR***") under U.S. federal securities laws. In general, Regulation BTR prohibits any director or executive from engaging in certain transactions involving the Company's securities during periods when 401(k) plan participants are prevented from purchasing, selling or otherwise acquiring or transferring an interest in certain securities held in individual account plans. Any profits realized from a transaction that violates Regulation BTR are recoverable by the Company, regardless of the intentions of the director or executive effecting the transaction. In addition, individuals who engage in such transactions are subject to sanction by the SEC as well as potential criminal liability.

The Company will notify directors and executives if they are subject to a blackout trading restriction under Regulation BTR. Failure to comply with an applicable trading blackout in accordance with Regulation BTR is a violation of law and this Policy.

8. Exceptions to the Insider Trading Policy

There are limited exceptions to this Policy, which are described below. Please note that there may be instances where you suffer financial harm or other hardship or are otherwise required to forgo a planned transaction because of the restrictions imposed by this Policy. Personal financial emergency or other personal circumstances are not mitigating factors under securities laws and will not excuse a failure to comply with this Policy.

(a) Receipt, Vesting, and Exercise of Stock Awards

The trading restrictions under this Policy do not apply to the acceptance or purchase of stock options, restricted stock or the like issued or offered directly by the Company, nor do they apply to the vesting, cancellation, forfeiture of stock options, restricted stock, restricted stock units or stock appreciation rights or the acquisition or repurchase of shares pursuant to option exercises under the Company's option plans. This exception applies solely to the receipt or forfeiture of equity awards or common stock to or from the Company. Transfers of shares or equity awards in the open market, including to cover tax withholding obligations, are addressed in Section 8(b) below and are subject to further limitations.

(b) Sale of Shares to Cover Tax Withholdings

The trading restrictions under this Policy do not apply to the sale of shares of the Company's common stock issued upon vesting of restricted stock units for the limited purpose of covering tax withholding obligations (and any associated broker or other fees), provided that, if required by the Compliance Officer, prior to such sale you elect to sell such shares to cover tax withholding obligations in a manner approved by a Compliance Officer or such sale is effected pursuant to a sell-to-cover program mandated by the Company.

(c) Tax Withholding Transactions. This policy does not apply to the surrender of shares directly to the Company to satisfy tax withholding obligations as a result of the issuance of shares upon vesting or exercise of restricted stock units, options, or other equity awards

granted under the Company's equity compensation plans. Of course, any market sale of the stock received upon exercise or vesting of any such equity awards remains subject to all provisions of this policy whether or not for the purpose of generating the cash needed to pay the exercise price or pay taxes.

(d) Purchases from the Company's Employee Stock Purchase Plan

The trading restrictions under this Policy do not apply to elections with respect to participation in any employee stock purchase plan or to purchases of the Company's common stock under such plan. However, the trading restrictions do apply to subsequent sales of the Company's common stock.

(e) Stock Splits, Stock Dividends and Similar Transactions

The trading restrictions under this Policy do not apply to a change in the number of securities held as a result of a stock split or stock dividend applying equally to all securities of a class, or similar transactions.

(f) 10b5-1 Plans

The SEC has enacted rules that provide an affirmative defense against alleged violations of U.S. federal insider trading laws for transactions made pursuant to trading plans that meet certain requirements, commonly referred to as "10b5-1 trading plans." These trading plans must be entered into, amended, modified or terminated, when participants are not aware of material nonpublic information, during an open trading window (as described in Section 6(i)), meet the requirements set forth in Rule 10b5-1 of the Securities Exchange Act of 1934, as amended ("Rule 10b5-1") and meet those specific requirements or guidelines established by the Company for such plans. In addition, these trading plans, including any amendment, modification or termination, must be pre-approved, in writing, by a Compliance Officer or Compliance Officer's delegate(s). Transactions made pursuant to a 10b5-1 trading plan are not subject to the restrictions in this Policy, even if you are aware of material nonpublic information at the time of the transaction or a blackout period is in effect.

Executives and directors, and persons identified on Schedule I hereto, are encouraged, should they wish to trade in the Company's common stock, to do so via a 10b5-1 Plan, subject to such plan complying with Rule 10b5-1 and meeting those specific requirements or guidelines established by the Company for such plans, including as set forth in the Company's 10b5-1 Plan Guidelines. Trading plans must be pre-approved by and filed with a Compliance Officer.

(g) Other Exceptions

Any other exception from this Policy must be approved by a Compliance Officer in consultation with the Nominating and Corporate Governance Committee of the Board.

Please be aware that even if a transaction falls within one of the exceptions described above, you will need to separately assess whether the transaction complies with applicable law. If you have any questions, please consult with a Compliance Officer.

9. Consequences of Insider Trading

Penalties for violating insider trading laws can include disgorging profit made or loss avoided by trading, paying the loss suffered by the persons who purchased securities from, or sold securities to, the insider tippee, paying civil and/or criminal penalties, and/or serving a jail term. the Company and/or supervisors of the person violating the rules may also be required to pay civil or criminal penalties and could be subject to private lawsuits.

A violation of this Policy is not necessarily a violation of law. In fact, for reasons explained in this Policy, it is not necessary for us to wait for the filing or conclusion of any civil or criminal action against an alleged violator before taking disciplinary action as your employer. In addition, please remember that the Company may prohibit a transaction from being completed to enforce compliance with this Policy.

10. How to Report Violations of the Insider Trading Policy

Please promptly report violations or suspected violations of this Policy to a Compliance Officer. You may also report via the Company's EthicsPoint helpline at www.rubrik.ethicspoint.com.

11. Policy's Duration

This Policy applies to you even after your relationship with the Company has ended. If you possess material nonpublic information when your relationship with the Company ends, you may not trade in the Company's stock or the stock of other companies to which such information relates until the material nonpublic information is publicly known or is no longer material. Further, if you leave the Company during a quarterly blackout period, then you may not trade the Company's securities until such quarterly blackout period has ended.

12. Priority of Statutory or Regulatory Trading Restrictions

The trading prohibitions and restrictions set forth in this Policy will be superseded by any greater prohibitions or restrictions prescribed by federal or state securities laws and regulations, or contractual restrictions on the sale of securities.

13. Amendments

The Company reserves the right to amend this Policy at any time, for any reason, subject to applicable law.

Exhibit 21.1

Subsidiaries of Rubrik, Inc.

Name	**Jurisdiction of Organization**
Rubrik India Private Limited	India

Exhibit 23.1

Consent of Independent Registered Public Accounting Firm

We consent to the incorporation by reference in the registration statement (No. 333-278434) on Form S-1, and in the registration statements (Nos. 333-278923 and 333-278922) on Form S-8, of our report dated March 20, 2025, with respect to the consolidated financial statements of Rubrik, Inc.

/s/ KPMG LLP

Santa Clara, California
March 20, 2025

Exhibit 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

I, Bipul Sinha, certify that:

1. I have reviewed this Annual Report on Form 10-K 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)) 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. 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
    c. 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: March 20, 2025

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

Exhibit 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

I, Kiran Choudary, certify that:

1. I have reviewed this Annual Report on Form 10-K 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)) 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. 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
    c. 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: March 20, 2025

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

Exhibit 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

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 Annual Report on Form 10-K of the Company for the period ended January 31, 2025 (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: March 20, 2025

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

This certification accompanies the Form 10-K 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-K), irrespective of any general incorporation language contained in such filing.

Exhibit 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

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 Annual Report on Form 10-K of the Company for the period ended January 31, 2025 (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: March 20, 2025

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

This certification accompanies the Form 10-K 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-K), irrespective of any general incorporation language contained in such filing.

Exhibit 97.1

Rubrik, Inc.

Incentive Compensation Recoupment Policy

1. Introduction

The Board of Directors (the "***Board***") of Rubrik, Inc., a Delaware corporation (the "***Company***"), has determined that it is in the best interests of the Company and its stockholders to adopt this Incentive Compensation Recoupment Policy (this "***Policy***") providing for the Company's recoupment of Recoverable Incentive Compensation that is received by Covered Officers of the Company under certain circumstances. Certain capitalized terms used in this Policy have the meanings given to such terms in Section 3 below.

This Policy is designed to comply with, and shall be interpreted to be consistent with, Section 10D of the Exchange Act, Rule 10D-1 promulgated thereunder ("***Rule 10D-1***") and Section 303A.14 of the New York Stock Exchange Listed Company Manual (the "***Listing Standards***").

2. Effective Date

This Policy shall apply to all Incentive Compensation that is received by a Covered Officer on or after April 25, 2024 (the "***Effective Date***"). Incentive Compensation is deemed "***received***" in the Company's fiscal period in which the Financial Reporting Measure specified in the Incentive Compensation award is attained, even if the payment or grant of such Incentive Compensation occurs after the end of that period.

3. Definitions

"***Accounting Restatement***" means an accounting restatement that the Company is required to prepare due to the material noncompliance of the Company with any financial reporting requirement under the securities laws, including any required accounting restatement to correct an error in previously issued financial statements that is material to the previously issued financial statements, or that would result in a material misstatement if the error were corrected in the current period or left uncorrected in the current period.

"***Accounting Restatement Date***" means the earlier to occur of (a) the date that the Board, a committee of the Board authorized to take such action, or the officer or officers of the Company authorized to take such action if Board action is not required, concludes, or reasonably should have concluded, that the Company is required to prepare an Accounting Restatement, or (b) the date that a court, regulator or other legally authorized body directs the Company to prepare an Accounting Restatement.

"***Administrator***" means the Compensation Committee or, in the absence of such committee, the Board.

"***Code***" means the U.S. Internal Revenue Code of 1986, as amended, and the regulations promulgated thereunder.

"***Compensation Committee***" means the Compensation Committee of the Board.

"***Covered Officer***" means each current and former Executive Officer.

"***Exchange***" means the New York Stock Exchange.

"***Exchange Act***" means the U.S. Securities Exchange Act of 1934, as amended.

"***Executive Officer***" means the Company's president, principal financial officer, principal accounting officer (or if there is no such accounting officer, the controller), any vice-president of the Company in charge of a principal business unit, division, or function (such as sales, administration, or finance), any other officer who performs a policy-making function, or any other person who performs similar policy-making functions for the Company. Executive officers of the Company's parent(s) or subsidiaries are deemed executive officers of the Company if they perform such policy-making functions for the Company. Policy-making function is not intended to include policy-making functions that are not significant. Identification of an executive officer for purposes of this Policy would include at a minimum executive officers identified pursuant to Item 401(b) of Regulation S-K promulgated under the Exchange Act.

"***Financial Reporting Measures***" means measures that are determined and presented in accordance with the accounting principles used in preparing the Company's financial statements, and any measures derived wholly or in part from such measures, including Company stock price and total stockholder return ("***TSR***"). A measure need not be presented in the Company's financial statements or included in a filing with the SEC in order to be a Financial Reporting Measure.

"***Incentive Compensation***" means any compensation that is granted, earned or vested based wholly or in part upon the attainment of a Financial Reporting Measure.

"***Lookback Period***" means the three completed fiscal years immediately preceding the Accounting Restatement Date, as well as any transition period (resulting from a change in the Company's fiscal year) within or immediately following those three completed fiscal years (except that a transition period of at least nine months shall count as a completed fiscal year). Notwithstanding the foregoing, the Lookback Period shall not include fiscal years completed prior to the Effective Date.

"***Recoverable Incentive Compensation***" means Incentive Compensation received by a Covered Officer during the Lookback Period that exceeds the amount of Incentive Compensation that would have been received had such amount been determined based on the Accounting Restatement, computed without regard to any taxes paid (*i.e.*, on a gross basis without regard to tax withholdings and other deductions). For any compensation plans or programs that take into account Incentive Compensation, the amount of Recoverable Incentive Compensation for purposes of this Policy shall include, without limitation, the amount contributed to any notional account based on Recoverable Incentive Compensation and any earnings to date on that notional amount. For any Incentive Compensation that is based on stock price or TSR, where the Recoverable Incentive Compensation is not subject to mathematical recalculation directly from the information in an Accounting Restatement, the Administrator will determine the amount of Recoverable Incentive Compensation based on a reasonable estimate of the effect of the Accounting Restatement on the stock price or TSR upon which the Incentive Compensation was received. The Company shall maintain documentation of the determination of that reasonable estimate and provide such documentation to the Exchange in accordance with the Listing Standards.

"***SEC***" means the U.S. Securities and Exchange Commission.

4. Recoupment

(a) Applicability of Policy. This Policy applies to Incentive Compensation received by a Covered Officer (i) after beginning services as an Executive Officer, (ii) who served as an Executive Officer at any time during the performance period for such Incentive Compensation, (iii) while the Company had a class of securities listed on a national securities exchange or a national securities association, and (iv) during the Lookback Period.

(b) Recoupment Generally. Pursuant to the provisions of this Policy, if there is an Accounting Restatement, the Company must reasonably promptly recoup the full amount of the Recoverable Incentive Compensation, unless the conditions of one or more subsections of Section 4(c) of this Policy are met and the Compensation Committee, or, if such committee does not consist solely of independent directors, a majority of the independent directors serving on the Board, has made a determination that recoupment would be impracticable. Recoupment is required regardless of whether the Covered Officer engaged in any misconduct and regardless of fault, and the Company's obligation to recoup Recoverable Incentive Compensation is not dependent on whether or when any restated financial statements are filed.

(c) Impracticability of Recovery. Recoupment may be determined to be impracticable if, and only if:

(i) the direct expense paid to a third party to assist in enforcing this Policy would exceed the amount of the applicable Recoverable Incentive Compensation; provided that, before concluding that it would be impracticable to recover any amount of Recoverable Incentive Compensation based on expense of enforcement, the Company shall make a reasonable attempt to recover such Recoverable Incentive Compensation, document such reasonable attempt(s) to recover, and provide that documentation to the Exchange in accordance with the Listing Standards; or

(ii) recoupment of the applicable Recoverable Incentive Compensation would likely cause an otherwise tax-qualified retirement plan, under which benefits are broadly available to employees of the Company, to fail to meet the requirements of Code Section 401(a)(13) or Code Section 411(a) and regulations thereunder.

(d) Sources of Recoupment. To the extent permitted by applicable law, the Administrator shall, in its sole discretion, determine the timing and method for recouping Recoverable Incentive Compensation hereunder, provided that such recoupment is undertaken reasonably promptly. The Administrator may, in its discretion, seek recoupment from a Covered Officer from any of the following sources or a combination thereof, whether the applicable compensation was approved, awarded, granted, payable or paid to the Covered Officer prior to, on or after the Effective Date: (i) direct repayment of Recoverable Incentive Compensation previously paid to the Covered Officer; (ii) cancelling prior cash or equity-based awards (whether vested or unvested and whether paid or unpaid); (iii) cancelling or offsetting against any planned future cash or equity-based awards; (iv) forfeiture of deferred compensation, subject to compliance with Code Section 409A; and (v) any other method authorized by applicable law or contract. Subject to compliance with any applicable law, the Administrator may effectuate recoupment under this Policy from any amount otherwise payable to the Covered Officer, including amounts payable to such individual under any otherwise applicable Company plan or program, *e.g.*, base salary, bonuses or commissions and compensation previously deferred by the Covered Officer. The Administrator need not utilize the same method of recovery for all Covered Officers or with respect to all types of Recoverable Incentive Compensation.

(e) No Indemnification of Covered Officers. Notwithstanding any indemnification agreement, applicable insurance policy or any other agreement or provision of the Company's certificate of incorporation or bylaws to the contrary, no Covered Officer shall be entitled to indemnification or advancement of expenses in connection with any enforcement of this Policy by the Company, including paying or reimbursing such Covered Officer for insurance premiums to cover potential obligations to the Company under this Policy.

(f) Indemnification of Administrator. Any members of the Administrator, and any other members of the Board who assist in the administration of this Policy, shall not be personally liable for any action, determination or interpretation made with respect to this Policy and shall be indemnified by the Company to the fullest extent under applicable law and Company policy with respect to any such action, determination or interpretation. The foregoing sentence shall not limit any other rights to indemnification of the members of the Board under applicable law or Company policy.

(g) No "Good Reason" for Covered Officers. Any action by the Company to recoup or any recoupment of Recoverable Incentive Compensation under this Policy from a Covered Officer shall not be deemed (i) "good reason" for resignation or to serve as a basis for a claim of constructive termination under any benefits or compensation arrangement applicable to such Covered Officer, or (ii) to constitute a breach of a contract or other arrangement to which such Covered Officer is party.

5. Administration

Except as specifically set forth herein, this Policy shall be administered by the Administrator. The Administrator shall have full and final authority to make any and all determinations required under this Policy. Any determination by the Administrator with respect to this Policy shall be final, conclusive and binding on all interested parties and need not be uniform with respect to each individual covered by this Policy. In carrying out the administration of this Policy, the Administrator is authorized and directed to consult with the full Board or such other committees of the Board as may be necessary or appropriate as to matters within the scope of such other committee's responsibility and authority. Subject to applicable law, the Administrator may authorize and empower any officer or employee of the Company to take any and all actions that the Administrator, in its sole discretion, deems necessary or appropriate to carry out the purpose and intent of this Policy (other than with respect to any recovery under this Policy involving such officer or employee).

6. Severability

If any provision of this Policy or the application of any such provision to a Covered Officer shall be adjudicated to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect any other provisions of this Policy, and the invalid, illegal or unenforceable provisions shall be deemed amended to the minimum extent necessary to render any such provision or application enforceable.

7. No Impairment of Other Remedies

Nothing contained in this Policy, and no recoupment or recovery as contemplated herein, shall limit any claims, damages or other legal remedies the Company or any of its affiliates may have against a Covered Officer arising out of or resulting from any actions or omissions by the Covered Officer. This Policy does not preclude the Company from taking any other action to enforce a Covered Officer's obligations to the Company, including, without limitation, termination of employment and/or institution of civil proceedings. This Policy is in addition to the requirements of Section 304 of the Sarbanes-Oxley Act of 2002 ("***SOX 304***") that are applicable to the Company's Chief Executive Officer and Chief Financial Officer and to any other compensation recoupment policy and/or similar provisions in any employment, equity plan, equity award, or other individual agreement, to which the Company is a party or which the Company has adopted or may adopt and maintain from time to time; provided, however, that compensation recouped pursuant to this Policy shall not be duplicative of compensation recouped pursuant to SOX 304 or any such compensation recoupment policy and/or similar provisions in any such employment, equity plan, equity award, or other individual agreement except as may be required by law.

8. Amendment; Termination

The Administrator may amend, terminate or replace this Policy or any portion of this Policy at any time and from time to time in its sole discretion. The Administrator shall amend this Policy as it deems necessary to comply with applicable law or any Listing Standard.

9. Successors

This Policy shall be binding and enforceable against all Covered Officers and, to the extent required by Rule 10D-1 and/or the applicable Listing Standards, their beneficiaries, heirs, executors, administrators or other legal representatives.

10. Required Filings

The Company shall make any disclosures and filings with respect to this Policy that are required by law, including as required by the SEC.

* * * * *

Rubrik, Inc.

Incentive Compensation Recoupment Policy

Form of Executive Acknowledgment

I, the undersigned, agree and acknowledge that I am bound by, and subject to, the Rubrik, Inc. Incentive Compensation Recoupment Policy, as may be amended, restated, supplemented or otherwise modified from time to time (the "***Policy***"). In the event of any inconsistency between the Policy and the terms of any employment agreement, offer letter or other individual agreement with Rubrik, Inc. (the "***Company***") to which I am a party, or the terms of any compensation plan, program or agreement, whether or not written, under which any compensation has been granted, awarded, earned or paid to me, the terms of the Policy shall govern.

In the event that the Administrator (as defined in the Policy) determines that any compensation granted, awarded, earned or paid to me must be forfeited or reimbursed to the Company pursuant to the Policy, I will promptly take any action necessary to effectuate such forfeiture and/or reimbursement. I further agree and acknowledge that I am not entitled to indemnification, and hereby waive any right to advancement of expenses, in connection with any enforcement of the Policy by the Company.

Agreed and Acknowledged:

__

Name: __

Title: __

Date: __