Risk Factors Comparison 2025-02-18 to 2024-02-21 Form: 10-K

Legend: **New Text** ~~Removed Text~~ Unchanged Text Moved Text Section

On December 2, 2024, we completed our acquisition of the University of St. Augustine for Health Sciences (" USAHS "). Our future success will depend, in part, on our ability to integrate USAHS, and any other institutions or businesses we may acquire in the future, into our operations. The successful integration and profitable operation of an acquired institution or business, including the realization of anticipated cost savings and additional revenue opportunities, can present challenges, and the failure to overcome these challenges can have an adverse effect on our business, financial condition, cash flows and results of operations. **Such** ~~Some of these~~ challenges **, while ultimately dependent on the particular acquisition at hand, may** include ~~: The~~ **, among other things, the** inability to maintain uniform standards, controls, policies and procedures **; the acquired business not performing as expected** ; distraction of management' s attention from normal business operations during the integration process; the inability to attract and / or retain key management personnel to operate the acquired entity; the inability to obtain, or ~~delay~~ **delays** in obtaining, regulatory or other approvals necessary to operate the business **; the risk that disruptions from the integration will harm our or the acquired entity' s businesses; potential adverse reactions or changes to business relationships resulting from the acquisition** ; the inability to correctly estimate the size of a target market or accurately assess market dynamics; expenses associated with the integration efforts; and ~~unidentified~~ **our assumption of unexpected risks, liabilities and obligations of the acquired business, including** issues not discovered in the due diligence process ~~, including legal contingencies~~ . An acquisition related to an institution or other educational business often requires various regulatory approvals **and in the case of a Title IV eligible institution, like USAHS, has recently required growth restrictions, reporting obligations and temporary conditions on operations that limit changes to the institution after acquisition** . If we are unable to obtain such approvals, or we obtain them on unfavorable terms, our ability to consummate a **future** transaction may be impaired or we may be unable to operate the acquired entity in a manner that is favorable to us. If we fail to properly evaluate an acquisition, we may be required to incur costs in excess of what we anticipated, and we may not achieve the anticipated benefits of such acquisition **, including the acquisition of USAHS. Natural disasters or other extraordinary events may cause us to close some of our schools or suffer casualty losses. We may experience business interruptions or casualty losses resulting from natural disasters, inclement weather, transit disruptions or other events in one or more of the geographic areas in which we operate, particularly in California, Colorado, Florida, Georgia and Texas, where our physical campuses are located. These events could impair the value of our assets and / or cause us to close physical campuses, temporarily or permanently, and could affect student recruiting opportunities in those locations, causing enrollment and revenue to decline, which could have a material adverse effect on our business, financial condition, results of operations and cash flows** . Risks Related to Our Business Technology Infrastructure If we, our third- party vendors, our regulators or any other quasi- governmental organization we are required to report information to are subject to cyberattacks, data breaches or other security incidents, or if there is a disruption or failure of our information technology systems or software, such events could expose us to liability and could adversely affect our financial condition and operating results. As part of our business, we collect, process, use ~~,~~ and store sensitive data and certain personal information from our students and employees. We also utilize third- party vendors and provide information about our students and employees to governmental and quasi- governmental external agencies to satisfy different legal and regulatory requirements and use electronic payment methods to process and store some of this information, including credit card information. Our business relies on information technology networks and systems to store this data, process financial and personal information, manage a variety of business processes, and comply with regulatory, legal and tax requirements. Additionally, we maintain other confidential, proprietary or otherwise sensitive information relating to our business and from third parties. The information technology networks and systems owned, operated, controlled or used by us, our third- party vendors or other external agencies may be vulnerable to damage, disruptions or shutdowns, software or hardware vulnerabilities, data breaches, security incidents, failures during the process of upgrading or replacing software or databases or components thereof, power outages, natural disasters, hardware failures, attacks by computer hackers, telecommunication failures, user errors, user malfeasance, computer viruses, unauthorized access, phishing or social engineering attacks, ransomware attacks, distributed denial- of- service attacks, brute force attacks, robocalls and other real or perceived cyberattacks or catastrophic events, all of which may not be prevented by our efforts to secure our networks and systems. Security incidents can also occur as a result of non- technical issues, including intentional or inadvertent actions by our employees, our third- party vendors, external agencies or their personnel, or other parties. Security incidents are becoming increasingly prevalent and severe, as well as increasingly difficult to detect. Any of these incidents could lead to interruptions or shutdowns of our platforms, disruptions in our ability to process service requests ~~,~~ **and** record or analyze the use of our services, **the** loss or corruption of data ~~,~~ or unauthorized access to, or acquisition of, personal information or other sensitive information, such as our intellectual property. We maintain policies and practices and operational safeguards, measures and controls aimed at reducing our cyber risk, protecting and recovering our data and ensuring business continuity, which include reasonable efforts **that aim** to ensure that our third- party vendors maintain reasonable security, including encryption and authentication technology, and will notify us promptly if a security incident occurs. However, none of our or our vendors' or external agencies' security measures can provide absolute security. Advances in computer capabilities, increasingly sophisticated tools and methods used by hackers and cyber terrorists, new discoveries in the field of cryptography or other developments may result in our failure or inability, or the failure or inability of our vendors or external agencies, to adequately protect personal or other sensitive information, and there can be no assurance that we, our vendors or

external agencies will not suffer a cyberattack, that hackers or other unauthorized parties will not gain access to or exfiltrate personal information or other sensitive data or that any such data compromise or unauthorized access will be discovered in a timely fashion. Like many businesses, we, our third- party vendors and external agencies have in the past and will in the future continue to be subject to cyberattacks, cybersecurity threats and attempts to compromise and penetrate our data security and systems and disrupt our services. Regular patching of each of our respective computer systems and frequent updates to our virus detection and prevention software with the latest virus and malware signatures may not catch newly introduced malware, ransomware, viruses or " zero- day " viruses prior to their infecting our, our third- party vendors and / or external agencies' computer systems or networks. Future cyberattacks against us, our third- party vendors or external agencies could lead to operational disruptions that could have an adverse effect on our ability to provide services to **students** ~~clients and customers~~ and on our results of operations and financial results. Any general decline in ~~Internet~~ **internet** use for any reason, including security or privacy concerns, cost of ~~Internet~~ **internet** service or changes in government regulation, could result in less demand for online educational services and inhibit growth in our online programs. Failure of our systems to operate effectively or a compromise in the security of our systems, or the systems of our ~~affiliates~~ **third- party vendors, external agencies** or other third parties, that results in unauthorized persons or entities obtaining personal information or other sensitive information could materially and adversely affect our reputation, operations, operating results and financial condition. Actual or anticipated cyberattacks may cause us to incur costs, including costs to deploy additional personnel and protection technologies, train employees, pay higher insurance premiums and engage third- party specialists for additional services. Breaches in our data security or that of our ~~affiliates~~ **third- party vendors, external agencies** or other third parties could expose us to risks of data loss, inappropriate disclosure of confidential or proprietary information, potential claims, investigations, regulatory proceedings, litigation penalties and liability, could impede our processing of transactions and our financial reporting and could result in a disruption of our operations. In addition, we may incur other substantial costs in connection with remediating and otherwise responding to any data security incident, including potential liability for stolen client, student or employee data, repairing system damage, or providing credit monitoring or other benefits to clients, students or employees affected by the incident. Additionally, if we, our third- party service providers or external agencies experience security incidents that result in a decline in performance of necessary services, availability problems or the loss, corruption of, unauthorized access to or disclosure of personal data or confidential information, people may become unwilling to provide us the information necessary to receive our services, and our reputation and market position could be harmed. Existing students may also decrease their use of our services or cease using our services altogether. The impact of ~~these~~ security threats, incidents and other disruptions are difficult to predict. Our insurance coverage for such security threats, incidents and other disruptions may not be adequate to cover all related costs, and we may not otherwise be fully indemnified for them. This may result in an increase in our costs for insurance or insurance not being available to us on economically feasible terms or at all. Insurers may also deny us coverage as to any future claim. Any of these results could **materially** harm our growth prospects, financial condition, business and reputation. The personal information that we collect may be vulnerable to breach, theft or loss **, any of** which could adversely affect our reputation, operations and ability to attract and retain students. In the ordinary course of our business, we maintain on our network systems **and** ~~, on~~ the networks of our third- party providers, and ~~have reported~~ -- **report** to external agencies **,** certain information that is confidential, proprietary, personal (such as student information) ~~,~~ or otherwise sensitive in nature, including financial information and confidential business information. Our computer networks, those of our vendors that manage confidential information for us or provide services to our students or us and those of external agencies can be accessed globally through the internet and are vulnerable to unauthorized access, inadvertent access or display, theft or misuse, hackers, installation of ransomware and malware and computer viruses, during regular use and in connection with hardware and software upgrades and changes. These attacks have become more prevalent and sophisticated. Unauthorized access, misuse, theft or hacks can evade our intrusion detection and prevention precautions **, and the intrusion detection and prevention precautions of our third- party providers and external agencies to which we report certain information,** without alerting us to the breach or loss for some period of time or ~~may never~~ **ever** ~~be detected~~. ~~A user who~~ **An individual or group that** circumvents security measures could misappropriate confidential or proprietary information or personal information about our students or employees, cause interruptions or malfunctions in **our** operations or commit fraud. We have experienced malware and virus attacks on our systems which went undetected by our virus detection and prevention software. The FTC passed an amendment to the Safeguards Rule under the Gramm- Leach- Bliley Act (~~"~~ **the "** GLBA ~~"~~ **"**), effective on June 9, 2023, that updated data security requirements for financial institutions, including all Title IV institutions of higher education. The Department has increased enforcement authority by requiring auditors to verify an institution' s compliance with components of the Safeguards Rule. ~~If the Department determines that an institution has not implemented a compliant information security program with the required elements by December 31, 2023, the institution would receive an audit finding and must submit a corrective action plan.~~ Failure to comply with the applicable GLBA requirements may result in FTC enforcement, which could include the imposition of conditions, penalties, monitoring and oversight. In addition to being subject to privacy and information security laws and regulations in the U. S., because our services can be accessed globally via the ~~Internet~~ **internet** , we may also be subject to privacy **and information security** laws in countries outside the U. S. from which students access our services, which laws may constrain the way we market and provide our services. Any breach of student or employee privacy or errors in storing, using or transmitting personal information could violate privacy laws and regulations resulting in fines or other penalties. The adoption of new or modified state or federal data or cybersecurity legislation could increase our costs and require changes in our operating procedures or systems. An example of this is the California Consumer Privacy Act which became effective January 1, 2020. The reliability of our program infrastructure and mechanisms to protect the personal information of our students is critical to our operations, reputation and ability to attract and retain students. A breach, theft or loss of personal information held by us, our vendors or an external agency, or a violation of the laws and regulations governing privacy, could have a material adverse effect

on our reputation and ability to attract and retain students, or result in lawsuits, additional regulation, remediation and compliance costs or investments in additional security systems to protect our computer networks, the costs of which may be substantial. Our **primarily** remote work environment may exacerbate the risks related to our business technology infrastructure. ~~Almost all~~ **A significant portion** of our employees work remotely, as do a number of our third- party service vendors. This remote work environment may exacerbate certain risks to our business, including increasing the stress on, and our vulnerability to disruptions of, our ~~technology~~ **technological** infrastructure and systems and the risks of phishing and other cybersecurity attacks, unauthorized dissemination of confidential information and social engineering attempts. If a natural disaster, power outage, connectivity issue or other event occurs that impacts the ability of employees to work remotely, it may be difficult or, in certain cases, impossible for us to continue our business for a period of time, which could ~~be substantial~~ **materially harm our growth prospects, financial condition, business and reputation** . Risk Related to Our Common Stock The trading price of our common stock may continue to fluctuate substantially in the future, and as a result returns on an investment in our common stock may be volatile. The trading price of our common stock has previously and may continue to fluctuate significantly as a result of a number of factors, some of which are not in our control. These factors **may** include: • the actual, anticipated or perceived impact of changes in the political environment or government policies; • the outcomes and impacts on our business of the Department' s rulemakings, and other changes in the legal or regulatory environment in which we operate; • negative media coverage of the for- profit education industry; • general economic conditions or conditions in the postsecondary education field, including declining enrollments; • the initiation, pendency or outcome of litigation, accreditation reviews, regulatory reviews, inquiries and investigations ~~,~~ and any related adverse publicity; • **the** failure of certain of our institutions or programs to maintain compliance under the 90- 10 Rule or other regulatory standards; • our ability to meet or exceed, or changes in, expectations of analysts or investors, or the extent of analyst coverage of our company; • any reduction or elimination of **our payment of** dividends **on our common stock** ; • decisions by any significant investors to reduce their investment in us; • quarterly variations in our operating results, which sometimes occur due to the academic calendar and significant expense items that do not regularly occur; • loss of key personnel; and • price and volume fluctuations in the overall stock market, which may cause the market price for our common stock to fluctuate significantly more than the market as a whole. Changes in the trading price of our common stock may occur without regard to our operating performance, and the price of our common stock could fluctuate based upon factors that have little or nothing to do with our company. Further, the trading volume of our common stock ~~is~~ **has historically been, and may continue to be,** relatively low, which may cause our stock price to react more to the above and other factors. The fluctuations in the trading price of our common stock may impact an investor' s ability to sell their shares at a desired time or at a price considered satisfactory, including at or above the price at which the investor acquired them. ~~You~~ **Shareholders** may not receive the level of dividends previously provided under the dividend policy our Board of Directors has adopted, or any dividends at all. We declared our first quarterly cash dividend in the third quarter of 2023 and have paid a quarterly dividend since then. However, we are not obligated to pay dividends on our common stock. Despite our history of paying dividends, the declaration and payment of all future dividends to holders of our common stock are subject to the discretion of our Board of Directors, which may amend, revoke or suspend our dividend policy at any time and for any reason, including earnings and cash flows, capital spending plans, financial conditions and other factors our Board of Directors may deem relevant. The terms of our indebtedness and any limitations imposed by regulatory authorities, among other factors, may also restrict us from paying cash dividends on our common stock under certain circumstances. Over time, our capital and other cash needs may change significantly from our current needs, which could affect whether we pay dividends and the level of any dividends we may pay in the future. Accordingly, ~~you~~ **shareholders** may not receive dividends ~~in~~ **consistent with** the previously issued amounts, or at all. Any reduction or elimination of dividends may cause the market price of our common stock to decline.