infrastructure and applications as part of ongoing cybersecurity management and in accordance with required regulatory practices. Any observations are ranked by severity and prioritized for response and remediation.

Our cybersecurity risk management extends to risks associated with our use of third-party service providers. We evaluate vendor security through an integrated process with our legal team to assess security and privacy risks to the business. This integrated process helps ensure appropriate contract provisions and complementary controls are in place to protect our and our customers' data. We execute this review process as we onboard a new vendor or renew a contract with an existing vendor, or when there are significant changes in the scope of services provided by the vendor. Key vendors are reassessed annually to confirm their control environment remains secure and meets our expectations.

Our platform is continuously probed and attacked by malicious actors, and accordingly, the controls and practices utilized by our cybersecurity and technology teams have continued to evolve. We utilize a Security Information and Event Management (SIEM) tool and Security Operations Center (SOC) provider to actively support our ability to monitor, alert, and remediate issues on a continuous basis and to protect our company from material security breaches or unauthorized access to our environment. Additionally, we employ a dedicated cybersecurity team to closely work with the SOC, key vendors, and internal stakeholders to maintain familiarity with our operations and configure systems to alert on risks to the organization using industry and business insights.

We closely monitor vendor and industry alerts to identify potential vulnerabilities and risks. These various threat and vulnerability alerts allow our cybersecurity team and trusted partners, such as hosting vendors and other critical service providers, to quickly respond to identified risks. Additionally, a periodic NIST-based risk assessment is performed by an independent third party to assist our cybersecurity team in confirming our cybersecurity control environment is in conformance with recognized cybersecurity industry frameworks and standards, as well as identifying any opportunities for enhancement. We also regularly train our employees on cybersecurity awareness, confidential information protection, and phishing attacks.

While we have not experienced any material cybersecurity threats or incidents in recent years, there can be no guarantee that we will not be the subject of future threats or incidents.

Like other companies, we are subject to cybersecurity threats and nonmaterial cybersecurity incidents from time to time. For example, in early February 2026, we identified a cybersecurity incident (the "Incident") in which an unauthorized third party gained access to certain of our systems by means of a social engineering attack on two employees. In response to the Incident, we promptly initiated our cybersecurity response plans and took steps to assess, contain, and remediate the unauthorized activity, including isolating the affected systems, launching an investigation with the assistance of external cybersecurity advisors, and coordinating with law enforcement. As of the date of this Annual Report on Form 10-K, we have confirmed that our customer service software platform was accessed and certain customer information was obtained. We have further confirmed that the vast majority of customer information accessed was limited to personally identifiable information (PII), specifically, names and email addresses, and less frequently phone numbers and physical addresses. Additionally, for customers who contacted customer service between mid-February 2025 and early February 2026 through our online customer service platform, the unauthorized third party may have gained access to customer data regarding category of treatment and other information included in their communications with customer service. Our electronic medical record was not accessed. When our investigation is complete, we will make required regulatory and individual notifications on a rolling basis. Our investigation into the Incident is ongoing, and we are still in the process of gathering details regarding the scope of information involved. While our investigation and assessment of the Incident is ongoing, as of the date of this Annual Report on Form 10-K, we do not believe the Incident is reasonably likely to materially impact our financial condition or results of operations. However, if new or additional information were to come to light as the investigation progresses, the impact of the incident could prove to be material to our business, financial condition, results of operations, or cash flows.

For a discussion of whether and how any risk from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect us, including our business strategy, results of operations, or financial condition, see Part I, Item 1A: "Risk Factors," which should be read in conjunction with this Part I, Item 1C.

Governance

Our Board of Directors maintains overall oversight of our risk management. The Audit Committee is specifically tasked with reviewing cybersecurity and other information technology risks, controls, and procedures, including our plans to mitigate