Cybersecurity and data privacy

We take data privacy and security seriously. We maintain policies and procedures designed to comply with applicable state and federal rules as well as employ the following measures:

Information security	We have policies and procedures for identifying, assessing and managing material risks associated with cybersecurity threats. To help protect our IT resources, we have instituted administrative, physical and technical controls and processes and commissioned third-party assessments. The technical defense measures we have implemented are designed to address vulnerabilities that may arise, including from a security control failure. These measures currently involve a combination of artificial intelligence; machine learning computer network monitoring; malware and antivirus resources; firewall systems; endpoint detection and response; cloud service defenses; Internet address and content filtering monitoring software intended to secure against known malicious websites and potential data exfiltration; and a variety of cyber intelligence and threat monitoring sources, which provide ongoing updates, all provided by third parties that we believe are capable of performing the service for which they have been engaged or governmental agencies. When engaging a third party for these types of services and resources, we typically conduct a security review involving, as relevant to the service or resource, discussions with the firm's security personnel, evaluation of auditor reports, and other requested information and documentation.
Employee education and awareness activities	To support the ongoing identification and management of cybersecurity issues, all employees are required to complete cybersecurity awareness training, including social engineering, password best practices, data classification and phishing awareness, with additional training for handling of customer personal information. We also publish a monthly security awareness newsletter along with performing ongoing internal phishing assessments.
Customer privacy	We do not sell our mailing or contact lists to unaffiliated third parties. KB Home may share customer email addresses and contact information with our selected service providers for home-related offers and other information that we believe may be of interest to our customers; however, customers are able to indicate on the guest information, registration card or other materials that they do not wish to be contacted.
Leadership oversight	Our Board of Directors, through its Audit and Compliance Committee, monitors cybersecurity risks and our evolving physical, electronic and other protection strategies and initiatives. Our management executives periodically review our cybersecurity practices and risks with the committee, most recently in January 2025.