The Company has invested and will continue to invest in programs to enhance reseller sales, including staffing selected resellers' stores with Company employees and contractors, and improving product placement displays. These programs can require a substantial investment while not assuring return or incremental sales. The financial condition of these resellers could weaken, these resellers could stop distributing the Company's products, or uncertainty regarding demand for some or all of the Company's products could cause resellers to reduce their ordering and marketing of the Company's products.

The Company's business and reputation are impacted by information technology system failures and network disruptions.

The Company and its global supply chain are dependent on complex information technology systems and are exposed to information technology system failures or network disruptions caused by natural disasters, accidents, power disruptions, telecommunications failures, acts of terrorism or war, computer viruses, physical or electronic break-ins, ransomware or other cybersecurity incidents, or other events or disruptions. System upgrades, redundancy and other continuity measures may be ineffective or inadequate, and the Company's or its vendors' business continuity and disaster recovery planning may not be sufficient for all eventualities. Such failures or disruptions can adversely impact the Company's business by, among other things, preventing access to the Company's online services, interfering with customer transactions or impeding the manufacturing and shipping of the Company's products. These events could materially adversely affect the Company's business, reputation, results of operations and financial condition.

Losses or unauthorized access to or releases of confidential information, including personal information, could subject the Company to significant reputational, financial, legal and operational consequences.

The Company's business requires it to use and store confidential information, including personal information, with respect to the Company's customers and employees. The Company devotes significant resources to network and data security, including through the use of encryption and other security measures intended to protect its systems and data. But these measures cannot provide absolute security, and losses or unauthorized access to or releases of confidential information occur and could materially adversely affect the Company's business, reputation, results of operations and financial condition.

The Company's business also requires it to share confidential information with suppliers and other third parties. The Company relies on global suppliers that are also exposed to ransomware and other malicious attacks that can disrupt business operations. Although the Company takes steps to secure confidential information that is provided to or accessible by third parties working on the Company's behalf, such measures are not always effective and losses or unauthorized access to, or releases of, confidential information occur. Such incidents and other malicious attacks could materially adversely affect the Company's business, reputation, results of operations and financial condition.

The Company experiences malicious attacks and other attempts to gain unauthorized access to its systems on a regular basis. These attacks seek to compromise the confidentiality, integrity or availability of confidential information or disrupt normal business operations, and can, among other things, impair the Company's ability to attract and retain customers for its products and services, impact the Company's stock price, materially damage commercial relationships, and expose the Company to litigation or government investigations, which could result in penalties, fines or judgments against the Company. Globally, attacks are expected to continue accelerating in both frequency and sophistication with increasing use by actors of tools and techniques that are designed to circumvent controls, avoid detection, and remove or obfuscate forensic evidence, all of which hinders the Company's ability to identify, investigate and recover from incidents. In addition, attacks against the Company and its customers can escalate during periods of severe diplomatic or armed conflict.

Although malicious attacks perpetrated to gain access to confidential information, including personal information, affect many companies across various industries, the Company is at a relatively greater risk of being targeted because of its high profile and the value of the confidential information it creates, owns, manages, stores and processes.

The Company has implemented systems and processes intended to secure its information technology systems and prevent unauthorized access to or loss of sensitive data, and mitigate the impact of unauthorized access, including through the use of encryption and authentication technologies. As with all companies, these security measures may not be sufficient for all eventualities and may be vulnerable to hacking, ransomware attacks, employee error, malfeasance, system error, faulty password management or other irregularities. For example, third parties can fraudulently induce the Company's or its vendors' employees or customers into disclosing usernames, passwords or other sensitive information, which can, in turn, be used for unauthorized access to the Company's or its vendors' systems and services. To help protect customers and the Company, the Company deploys and makes available technologies like multifactor authentication, monitors its services and systems for unusual activity and may freeze accounts under suspicious circumstances, which, among other things, can result in the delay or loss of customer orders or impede customer access to the Company's products and services.

While the Company maintains insurance coverage that is intended to address certain aspects of data security risks, such insurance coverage may be insufficient to cover all losses or all types of claims that may arise.