Company Response to Cybersecurity Risks

Increases in information technology ("IT") security threats and cyberattacks creates additional disruption risk to the Company's operations. The Company has implemented appropriate measures to address data security breaches and mitigate potential risks to the Company's IT systems.

The Audit Committee of the Company's Board of Directors has responsibility for the oversight of risk management activities related to IT security. The Company's Audit Committee is comprised of three independent directors, all of whom are financial experts. Senior management provides IT security updates and risk management action plans to the Audit Committee at least annually, and more frequently if considered necessary. Of the Company's seven current directors, six are considered independent.

Among the responsibilities listed in its Charter, the Company's Audit Committee is responsible for reviewing and discussing with management and the independent auditor the adequacy of the Company's internal controls and financial reporting controls. The Company's management is responsible for establishing and maintaining an adequate system of internal control over financial reporting, which includes controls over the Company's key IT systems. As part of its annual assessment, controls around IT system access, program change, and security are evaluated for effectiveness. Based on the most recent assessment completed, both management and the Company's Independent Registered Public Accounting Firm concluded that the Company's internal controls over financial reporting were effective.

The Company's management places reliance on the work of its Internal Audit department in making its assessment of the effectiveness of internal controls. To provide for the independence of the Company's Internal Audit department, its personnel report to the Company's Director of Internal Audit, who reports functionally to the Company's Audit Committee and administratively to the Chief Financial Officer.

As part of the Company's cybersecurity risk management process, the Company has implemented a variety of tools to assist employees in identifying potential threats and educating employees on information security best practices. The Company conducts quarterly information security training and compliance program and has also invested in software designed to identify potential threats.

The Company also engages third-party consultants with information security certifications to perform internal and external penetration tests, taking actions to address any recommended improvements, where applicable. The Company has entered into an information security risk insurance policy with a reputable insurance provider.

In the last three years, the Company has not experienced any significant information security breaches, and there were no expenses or fines related to breach penalties and settlements.

However, as new cyber threats emerge, the Company's systems and networks could be potentially vulnerable to new attacks. If the Company experiences a cyberattack that impairs its IT infrastructure, the resulting disruptions could impede the Company's ability to record or process orders, manufacture and ship products in a timely manner, or otherwise carry on business in the ordinary course. Any of these events could cause the loss of customers or revenue and could cause significant expense to be incurred to eliminate these problems and address related security concerns.