Mastercard and Visa ("EMV") card transactions. The Company completed the implementation of EMV technology and received certification in Fiscal 2018, however future upgrades to the Company's systems could expose the Company to the fraudulent use of credit cards and increased costs, including possible fines and restrictions on the Company's ability to accept payments by credit or debit cards, if the Company were not to receive recertification. Because we accept debit and credit cards for payment, we are also subject to industry data protection standards and protocols, such as the Payment Card Industry Data Security Standards (“PCI DSS”), issued by the Payment Card Industry Security Standards Council. Additionally, we have implemented technology in our stores to allow for the acceptance of EMV credit transactions and point-to-point encryption. Complying with PCI DSS standards and implementing related procedures, technology and information security measures require significant resources and ongoing attention. However, even if we comply with PCI DSS standards and offer EMV and point-to-point encryption technology in our stores, we may be vulnerable to, and unable to detect and appropriately respond to, data security breaches and data loss, including cybersecurity attacks or other breach of cardholder data.

In addition, the Payment Card Industry is controlled by a limited number of vendors who have the ability to impose changes in the Payment Card Industry’s fee structure and operational requirements on us without negotiation. Such changes in fees and operational requirements may result in our failure to comply with PCI DSS, and cause us to incur significant unanticipated expenses.

A privacy breach, through a cybersecurity incident or otherwise, or failure to comply with privacy laws could materially adversely affect our business.

As part of normal operations, we and our third-party vendors and partners, receive and maintain confidential and personally identifiable information about our customers and employees, and confidential financial, intellectual property, and other information. We regard the protection of our customer, employee, and company information as critical. The regulatory environment surrounding information security and privacy is very demanding, with the frequent imposition of new and changing requirements some of which involve significant costs to implement and significant penalties if not followed properly. Despite our efforts and technology to secure our computer network and systems, a cybersecurity breach, whether targeted, random, or inadvertent, and whether at the hands of cyber criminals, hackers, rogue employees or other persons, may occur and could go undetected for a period of time, resulting in a material disruption of our computer network, a loss of information valuable to our business, including without limitation customer or employee personally identifiable information, and/or theft. A similar cybersecurity breach to the computer networks and systems of our third-party vendors and partners, including those that are "cloud"-based, over which we have no control, may occur, and could lead to a material disruption of our computer network and/or the areas of our business that are dependent on the support, services and other products provided by our third-party vendors and partners. Our computer networks and our business may be adversely affected by such a breach of our third-party vendors and partners, which could result in a decrease in our e-commerce sales and/or a loss of information valuable to our business, including, without limitation, personally identifiable information of customers or employees. Such a cyber-incident could result in any of the following:

- theft, destruction, loss, misappropriation, or release of confidential financial and other data, intellectual property, customer awards or loyalty points, or customer or employee information, including personally identifiable information such as payment card information, email addresses, passwords, social security numbers, home addresses, or health information;
- operational or business delays resulting from the disruption of our e-commerce sites, computer networks or the computer networks of our third-party vendors and partners and subsequent material clean-up and mitigation costs and activities;
- negative publicity resulting in material reputation or brand damage with our customers, vendors, third-party partners or industry peers;
- loss of sales, including those generated through our e-commerce websites; and
- governmental penalties, fines and/or enforcement actions, payment and industry penalties and fines and/or class action and other lawsuits.

Any of the above risks, individually or in aggregation, could materially damage our reputation and result in lost sales, governmental and payment card industry fines, and/or class action and other lawsuits, which in turn could have a material adverse effect on our financial position, results of operations, and cash flows. Although we carry cybersecurity insurance, in the event of a cyber-incident, that insurance may not be extensive enough or adequate in scope of coverage or amount