Privacy Risk Study:

Loss of PII is Top Digital Risk for Public Companies

iapp.org
Executive summary

The U.S. Securities and Exchange Commission requires most publicly traded companies to annually disclose potential risk factors, including cybersecurity concerns. According to an IAPP study of the disclosure statements of more than 100 publicly traded companies, losing customers’ or employees’ personally identifiable information (PII) ranks first among disclosed information-related risks.

For those companies disclosing privacy risk, reputational harm is the greatest consequence of concern (83 percent), far more than the risk of civil litigation (60 percent), regulatory enforcement (51 percent), or remediation (50 percent).

Among other findings, it is also of note that 43 percent of companies that disclose privacy risks specify the risk of failing to comply with privacy laws and regulations, and 25 percent express concern about new laws, but only a handful of companies mention compliance with the European data protection framework or cross-border data transfer requirements. To be sure, these numbers may reflect the traditionally low likelihood of enforcement in Europe; and they may significantly change as the General Data Protection Regulation introduces the possibility of heavy fines in the amount of 4 percent of global turnover.

Finally, as an annex to this study, readers will find sample language used by selected companies in various industries to help them identify the emerging nomenclature of privacy risks.
Background and methodology

Pursuant to U.S. securities laws, companies that issue securities are required to file with the SEC annual reports that include a "Form 10-K." Companies generally file 10-Ks shortly after the close of their fiscal year, typically December 31.

Among the items to be disclosed on Form 10-K are the most significant factors that make the securities offered by the company speculative or risky to investors.

The Westin Research Center analyzed Form 10-K disclosures for 2015 filed by U.S. companies ranked in the top 150 by revenue according to Fortune magazine. We excluded from our research results companies that did not list digital information risks or file a 10K at all, and focused on the 114 companies whose Form 10-K disclosed digital risks.

We then categorized the disclosures made by these companies based upon their perceived privacy or security threats; the type of information companies felt was the most vulnerable; the companies' legal concerns; and the possible business harms associated with these privacy and security risks. We also categorized the companies by industry sector using S&P's Global Industry Classification Standard industry categories: energy, materials, industrials, consumer discretionary, consumer staples, health care, financials, information technology, telecommunications services, and utilities. The GICS's use of broad sector categories allows for robust comparisons between sectors and has the advantage of separating privacy-regulated industries, such as healthcare and financials, from less-regulated industries, such as consumer staples and IT.
Cybersecurity tops the list

We found that companies are far more concerned about cyber attack than any other information-related threat. Eighty-six percent of the companies disclosing privacy and security risks in their Form 10-K specify risk of hacking or cyber incidents. The next greatest concern is information mishandling by business partners, vendors, or other third parties (47 percent), which reinforces prior IAPP studies observing the growing role vendor management now plays in information privacy and security programs. Other concerns are damage to information technology systems themselves (45 percent), and employee misuse of data (43 percent). This last category may represent a considerable oversight: Many studies show employee error as the leading cause of data breaches.

Notable differences are apparent across industry sectors. Though companies in all sectors are most likely to list cyber-attacks among their 10-K risk disclosures, sectors differ in their likelihood to list third-party misuse among perceived threats. Companies in regulated sectors like healthcare and finance, for example, list risks associated with vendor vulnerabilities almost as frequently as they do threat of cyber attack. This supports regulation's role in shaping organizational attitudes toward information risks.

86% of the companies disclosing privacy and security risks in their Form 10-K specify risk of hacking or cyber incidents.
In contrast, companies in the information technology sector — and, indeed, most other sectors — are much less likely to specify third-party misuse as a significant threat. This is remarkable given the rise of information sharing between contracting companies as part of everyday business practice across industries. These findings could imply that regulated industries are more concerned with — and consequently perhaps more prepared for — risk of vendor or third-party data mishandling than others.

It will be interesting to see how the European Union’s sector-neutral General Data Protection Regulation, with its heavy emphasis on the controller-processor relationship, will affect organizational perspectives on third-party data handling risks when it comes into force in 2018.

The IAPP’s recent studies confirm that companies are indeed increasing their investments in privacy programs, including information security and vendor management.
PII risk outweighs IP concerns

Companies are most concerned about loss of PII — even when accounted for separately from protected health information (PHI) and payment card information (PCI); 61 percent of companies report that unauthorized disclosure of PII was a major risk factor for investors and potential investors, followed by disclosure of confidential information (54 percent). These numbers far exceed corporate concerns about loss of intellectual property or other proprietary information (45 percent). Although losing IP through cyber espionage puts companies at a disadvantage relative to their competitors, it does not necessarily expose them to liability, damage to reputation, or loss of consumer trust like a breach of PII.

Vulnerabilities: Loss of Protected Information

Number of surveyed 10-Ks listing risk of loss of this information type
Publicly traded U.S. companies are also alerting their investors to privacy legal compliance challenges — 43 percent of companies that disclose digital risks list a risk of failing to comply with existing privacy and data protection laws and regulations, while 25 percent express concern about the potential for new laws and regulations and the difficulty of keeping up with a constantly shifting legal landscape. Interestingly, only a small number of companies specifically mention compliance with international data protection laws, such as the European data protection framework, or cross-border data transfer requirements. This number could increase, however, now that the EU’s GDPR is coming into force and introducing hefty fines.

If a company specifies privacy law compliance concerns, it most likely lists “state consumer protection laws” (12 percent) or HIPAA / HI-TECH (10 percent), while another 10 percent of companies mention their obligations to comply with PCI security standards as a potential risk factor. But, generally speaking, Form 10-K disclosures discuss privacy and security risks in broad terms without mentioning specific statutes, regulations, or industry standards.

**Compliance Challenges**

<table>
<thead>
<tr>
<th>Compliance Challenge</th>
<th>Number of Companies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance with existing laws, regulations, contracts, and consent orders</td>
<td>49</td>
</tr>
<tr>
<td>Introduction of new laws and legal standards</td>
<td>29</td>
</tr>
<tr>
<td>Specific U.S. federal regulations (HIPAA, GLBA, etc.)</td>
<td>37</td>
</tr>
<tr>
<td>PCI standards or contracts</td>
<td>37</td>
</tr>
<tr>
<td>Specific European regulations (GDPR, Privacy Shield, etc.)</td>
<td>30</td>
</tr>
</tbody>
</table>

Form 10-K disclosures discuss privacy and security risks in broad terms.
Brand and reputation most vulnerable in breach

Companies present the potential for harm to their brand or reputation as the main source of risk as a result of losing PII or violating privacy legislation. Of the 114 companies that mention a privacy or security risk, 83 percent disclose concerns about reputational harm — a far greater number than those concerned with the risk of civil litigation (60 percent), regulatory enforcement (51 percent), costs of remediation (50 percent), or increased expenses on security systems and personnel (42 percent). Other possible risks include harm to relationships with consumers (39 percent) and business partners (24 percent).

One out of five companies warns investors that should it become subject to a data breach, its liability could exceed insurance coverage; the same percentage note that management and other personnel could be distracted from core business objectives.

Conclusion

The 2016 IAPP-EY Governance Report demonstrates that privacy issues have become board-level concern. In this first annual look at privacy risk disclosures in Form 10-K filings, we find U.S. companies are warning investors that protecting PII is a priority because disclosure could lead to reputational harm, and may adversely affect the bottom line.
Following are excerpts from Form 10K risk disclosures relating to information privacy concerns. We selected them for comprehensiveness, industry, global perspective, and in some cases use of phrases common to multiple disclosures. They have been edited for length, relevance and company identity.

**Simple compliance-based disclosure**

The Company's business is subject to a variety of U.S. and international laws, rules, policies and other obligations regarding data protection.

The Company is subject to federal, state and international laws relating to the collection, use, retention, security and transfer of PII. In many cases, these laws apply not only to third-party transactions, but also to transfers of information between the Company and its subsidiaries, and among the Company, its subsidiaries and other parties with which the Company has commercial relations. Several jurisdictions have passed laws in this area, and other jurisdictions are considering imposing additional restrictions. These laws continue to develop and may be inconsistent from jurisdiction to jurisdiction. Complying with emerging and changing international requirements may cause the Company to incur substantial costs or require the Company to change its business practices. Noncompliance could result in penalties or significant legal liability.

The Company's privacy policy, which includes related practices concerning the use and disclosure of data, is posted on its website. Any failure by the Company, its suppliers or other parties with whom the Company does business to comply with its posted privacy policy or with other federal, state or international privacy-related or data protection laws and regulations could result in proceedings against the Company by governmental entities or others.

The Company is also subject to payment card association rules and obligations under its contracts with payment card processors. Under these rules and obligations, if information is compromised, the Company could be liable to payment card issuers for associated expenses and penalties. In addition, if the Company fails to follow payment card industry security standards, even if no customer information is compromised, the Company could incur significant fines or experience a significant increase in payment card transaction costs.
Company A:

Cyber-attacks and security vulnerabilities could lead to reduced revenue, increased costs, liability claims, or harm to our competitive position. ...

Threats to IT security can take a variety of forms. Individual and groups of hackers, and sophisticated organizations including state-sponsored organizations or nation-states themselves, may take steps that pose threats to our customers and our IT. They may develop and deploy malicious software to attack our products and services and gain access to our networks and datacenters, or act in a coordinated manner to launch distributed denial of service or other coordinated attacks. Cyber threats are constantly evolving, thereby increasing the difficulty of detecting and successfully defending against them. Cyber threats can have cascading impacts that unfold with increasing speed across our internal networks and systems, and those of our partners and customers. Breaches of our network or data security could disrupt the security of our internal systems and business applications, impair our ability to provide services to our customers and protect the privacy of their data, result in product development delays, compromise confidential or technical business information harming our competitive position, result in theft or misuse of our intellectual property or other assets, require us to allocate more resources to improved technologies, or otherwise adversely affect our business.

In addition, our internal IT environment continues to evolve. Often we are early adopters of new devices and technologies. We embrace new ways of sharing data and communicating internally and with partners and customers using methods such as social networking and other consumer-oriented technologies. Our business policies and internal security controls may not keep pace with these changes as new threats emerge.
Security of our products, services, devices, and customers’ data. Security threats are a particular challenge to companies like us whose business is technology products and services. Threats to our own IT infrastructure can also affect our customers. Customers using our cloud-based services rely on the security of our infrastructure to ensure the reliability of our services and the protection of their data. Hackers tend to focus their efforts on the most popular operating systems, programs, and services, including many of ours, and we expect that to continue. The security of our products and services is important in our customers’ purchasing decisions.

To defend against security threats, both to our internal IT systems and those of our customers, we must continuously engineer more secure products and services, enhance security and reliability features, improve the deployment of software updates to address security vulnerabilities, develop mitigation technologies that help to secure customers from attacks even when software updates are not deployed, maintain the digital security infrastructure that protects the integrity of our network, products, and services, and provide customers security tools such as firewalls and anti-virus software.

The cost of these steps could reduce our operating margins. If we fail to do these things well, actual or perceived security vulnerabilities in our products and services could harm our reputation and lead customers to reduce or delay future purchases of products or subscriptions to services, or to use competing products or services. Customers may also spend more on protecting their existing computer systems from attack, which could delay adoption of additional products or services. Customers may fail to update their systems, continue to run software or operating systems we no longer support, or may fail timely to install security patches. Any of these actions by customers could adversely affect our revenue. Actual or perceived vulnerabilities may lead to claims against us. Although our license agreements typically contain provisions that eliminate or limit our exposure to liability, there is no assurance these provisions will withstand legal challenges. Legislative or regulatory action in these areas may increase the costs to develop, implement, or secure our products and services.

Disclosure of personal data could cause liability and harm our reputation. As we continue to grow the number and scale of our cloud-based offerings, we store and process increasingly large amounts of personally identifiable information of our customers. The continued occurrence of high-profile data breaches provides evidence of an external environment increasingly hostile to information security. Despite our efforts to improve the security controls across our business groups and geographies, it is possible our security controls over personal data, our training of employees and vendors on data security, and other practices we follow may not prevent the improper disclosure of customer data we or our vendors store and manage. Improper disclosure could harm our reputation, lead to legal exposure to customers, or subject us to liability under laws that protect personal data, resulting in increased costs or loss of revenue.
Our software products and services also enable our customers to store and process personal data on-premises or, increasingly, in a cloud-based environment we host. Government authorities can sometimes require us to produce customer data in response to valid legal orders. In the U.S. and elsewhere, we advocate for transparency concerning these requests and appropriate limitations on government authority to compel disclosure. Despite our efforts to protect customer data, perceptions that the privacy of personal information is not satisfactorily protected could inhibit sales of our products or services, and could limit adoption of our cloud-based solutions by consumers, businesses, and government entities. Additional security measures we may take to address customer concerns, or constraints on our flexibility to determine where and how to operate datacenters in response to customer expectations or governmental rules or actions, may cause higher operating expenses.

**Company B:**

If our security measures for our products and services are compromised and as a result, our data, our customers’ data or our IT systems are accessed improperly, made unavailable, or improperly modified, our products and services may be perceived as vulnerable, our brand and reputation could be damaged, the IT services we provide to our customers could be disrupted, and customers may stop using our products and services, all of which could reduce our revenue and earnings, increase our expenses and expose us to legal claims and regulatory actions. We are in the IT business, and our products and services, including our … Cloud offerings, store, retrieve, manipulate and manage our customers’ information and data, external data, as well as our own data. We have a reputation for secure and reliable product offerings and related services and we have invested a great deal of time and resources in protecting the integrity and security of our products, services and the internal and external data that we manage.

At times, we encounter attempts by third parties to identify and exploit product and service vulnerabilities, penetrate or bypass our security measures, and gain unauthorized access to our or our customers’, partners’ and suppliers’ software, hardware and cloud offerings, networks and systems, any of which could lead to the compromise of personal information or the confidential information or data of [company] or our customers. Computer hackers and others may be able to develop and deploy IT related viruses, worms, and other malicious software programs that could attack our products and services, exploit potential security vulnerabilities of our products and services, create system disruptions and cause shutdowns or denials of service. This is also true for third-party data, products or services incorporated into our own. Data may also be accessed or modified improperly as a result of customer, partner, employee or supplier error or malfeasance and third parties may attempt to fraudulently induce customers, partners,
Privacy Risk Study: Loss of PII Is Top Digital Risk for Public Companies

employees or suppliers into disclosing sensitive information such as user names, passwords or other information in order to gain access to our data, our customers’, suppliers’ or partners’ data or the IT systems of [company], its customers, suppliers or partners.

High-profile security breaches at other companies have increased in recent years, and security industry experts and government officials have warned about the risks of hackers and cyber-attacks targeting IT products and businesses. Although this is an industry-wide problem that affects other software and hardware companies, it affects [company] in particular because computer hackers tend to focus their efforts on the most prominent IT companies, and they may focus on [company] because of our reputation for, and marketing efforts associated with, having secure products and services. These risks will increase as we continue to grow our cloud offerings and store and process increasingly large amounts of data, including personal information and our customers’ confidential information and data and other external data, and host or manage parts of our customers’ businesses in cloud-based IT environments, especially in customer sectors involving particularly sensitive data such as health sciences, financial services and the government. We also have an active acquisition program and have acquired a number of companies, products, services and technologies over the years. While we make significant efforts to address any IT security issues with respect to our acquired companies, we may still inherit such risks when we integrate these companies within [company].

We could suffer significant damage to our brand and reputation if a cyber-attack or other security incident were to allow unauthorized access to or modification of our customers’ or suppliers’ data, other external data, or our own data or our IT systems or if the services we provide to our customers were disrupted, or if our products or services are perceived as having security vulnerabilities. Customers could lose confidence in the security and reliability of our products and services, including our cloud offerings, and perceive them to be not secure. This could lead to fewer customers using our products and services and result in reduced revenue and earnings. The costs we would incur to address and fix these security incidents would increase our expenses. These types of security incidents could also lead to lawsuits, regulatory investigations and claims and increased legal liability, including in some cases contractual costs related to customer notification and fraud monitoring.

Our business practices with respect to the collection, use and management of personal information could give rise to operational interruption, liabilities or reputational harm as a result of governmental regulation, legal requirements or industry standards relating to consumer privacy and data protection. As regulatory focus on privacy issues continues to increase and worldwide laws and regulations concerning the handling of personal information expand and become more complex, potential risks related to data collection and use within our business will intensify. For example, in October 2015, the Court
of Justice of the European Union (EU) invalidated the EU-U.S. Safe Harbor Framework, which [company] as well as many other global enterprises had relied on in certain contexts to enable the transfer of EU personal data to the United States. While [company] adapted to this judgment by implementing other transfer mechanisms permitted under applicable law, the validity of these other mechanisms could also be challenged. If successful, this could require [company] to make disruptive operational adjustments to the delivery of certain services that could impact customers and sales in the region. In addition, U.S. and foreign governments have enacted or are considering enacting legislation or regulations, or may in the near future interpret existing legislation or regulations, in a manner that could significantly impact the ability of [company] and our customers and data partners to collect, augment, analyze, use, transfer and share personal and other information that is integral to certain services [company] provides and data services. This could be true particularly in those jurisdictions where privacy laws or regulators take a broader view of how personal information is defined, therefore subjecting the handling of such data to heightened restrictions that may be obstructive to the operations of [company] and its customers and data providers. This impact may be acute in countries that have passed or are considering passing legislation that requires data to remain localized “in country,” as this imposes financial costs on any service provider that is required to store data in jurisdictions not of its choosing and nonstandard operational processes that are difficult and costly to integrate with global processes.

Regulators globally are also imposing greater monetary fines for privacy violations, and the EU is considering legislation that would impose fines for privacy violations based on a percentage of global revenues. Changes in laws or regulations associated with the enhanced protection of certain types of sensitive data, such as healthcare data or other personal information, could greatly increase our cost of providing our products and services or even prevent us from offering certain of our services in jurisdictions that we operate. Additionally, public perception and standards related to the privacy of personal information can shift rapidly, in ways that may affect [company]’s reputation or influence regulators to enact regulations and laws that may limit [company]’s ability to provide certain products. Any failure, or perceived failure, by [company] to comply with U.S. federal, state, or foreign laws and regulations, including laws and regulations regulating privacy, data security, or consumer protection, or other policies, public perception, standards, self-regulatory requirements or legal obligations, could result in lost or restricted business, proceedings, actions or fines brought against us or levied by governmental entities or others, or could adversely affect our business and harm our reputation.
Health care products/services sector

Company A:

Many of our activities involve the receipt, use and disclosure by us of personally identifiable information (“PII”) as permitted in accordance with applicable federal and state privacy and data security laws, which require organizations to provide appropriate privacy and security safeguards for such information. In addition to PII, we use and disclose de-identified data for analytical and other purposes when permitted. Additionally, there are industry standards for handling credit card data known as the Payment Card Industry Data Security Standard, which are a set of requirements designed to help ensure that entities that process, store or transmit credit card information maintain a secure environment. Certain states have recently incorporated these requirements into state laws.

The federal Health Insurance Portability and Accountability Act of 1996 and the regulations issued thereunder (collectively, “HIPAA”) impose extensive requirements on the way in which health plans, health care providers, health care clearinghouses (known as “covered entities”) and their business associates use, disclose and safeguard protected health information (“PHI”). Criminal penalties and civil sanctions may be imposed for failing to comply with HIPAA standards. The Health Information Technology for Economic and Clinical Health Act (the “HITECH Act”), enacted as part of the American Recovery and Reinvestment Act of 2009, amended HIPAA to impose additional restrictions on third-party funded communications using PHI and the receipt of remuneration in exchange for PHI. It also extended HIPAA privacy and security requirements and penalties directly to business associates. In addition to HIPAA, state health privacy laws apply to the extent they are more protective of individual privacy than is HIPAA.

Finally, the Health Insurance Marketplaces (formerly known as the “exchanges”) are required to adhere to privacy and security standards with respect to PII, and to impose privacy and security standards that are at least as protective of PII as those the Health Insurance Marketplace has implemented for itself or non-Health Insurance Marketplace entities, which include insurers offering plans through the Health Insurance Marketplaces and their designated downstream entities, including PBMs and other business associates. These standards may differ from, and be more stringent than, HIPAA.
The federal government has many consumer protection laws, such as the FTCA, the Federal Postal Service Act and the FTC’s Telemarketing Sales Rule. Most states also have similar consumer protection laws. These laws have been the basis for investigations, lawsuits and multi-state settlements relating to, among other matters, the marketing of loyalty programs and health care services, pricing accuracy, expired front store products, financial incentives provided by drug manufacturers to pharmacies in connection with therapeutic interchange programs and disclosures related to how personal data is used and protected.

**Company B:**

The Health Information Portability and Accountability Act of 1996 (“HIPAA”) and its accompanying federal regulations set forth privacy and security standards designed to protect the privacy of and provide for the security of individually identifiable health information, as such term is defined under the HIPAA regulations. Some of our businesses collect, maintain, and/or access individually identifiable health information and are subject to the HIPAA regulations. Our operations, depending on their location, may also be subject to state or foreign regulations affecting personal data protection and the manner in which information services or products are provided. Significant criminal and civil penalties may be imposed for violation of HIPAA standards and other such laws. We have a HIPAA compliance program to facilitate our ongoing effort to comply with the HIPAA regulations.

Enacted in 2009, the American Recovery and Reinvestment Act (“ARRA”) strengthens federal privacy and security provisions to protect individually identifiable health information. A section of the ARRA known as the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) strengthened certain aspects of the HIPAA privacy and security rules, imposed new notification requirements related to health data security breaches, broadened the rights of the U.S. Department of Health and Human Services (“HHS”) to enforce HIPAA, and directed HHS to publish more specific security standards. On January 25, 2013, the Office for Civil Rights of HHS published the HIPAA omnibus final rule (“HIPAA Final Rule”), which amended certain aspects of the HIPAA privacy, security and enforcement rules pursuant to the HITECH Act, extending certain HIPAA obligations to business associates and their subcontractors. Certain components of our business act as “business associates” within the meaning of HIPAA and are subject to these additional obligations under the HIPAA Final Rules.

Some of our businesses collect, maintain, and/or access other sensitive personal information that is subject to federal and state laws protecting such information, in addition to the requirements of HIPAA, the HITECH  

---

**ANNEX**

The federal government has many consumer protection laws, such as the FTCA, the Federal Postal Service Act and the FTC’s Telemarketing Sales Rule. Most states also have similar consumer protection laws. These laws have been the basis for investigations, lawsuits and multi-state settlements relating to, among other matters, the marketing of loyalty programs and health care services, pricing accuracy, expired front store products, financial incentives provided by drug manufacturers to pharmacies in connection with therapeutic interchange programs and disclosures related to how personal data is used and protected.

**Company B:**

The Health Information Portability and Accountability Act of 1996 (“HIPAA”) and its accompanying federal regulations set forth privacy and security standards designed to protect the privacy of and provide for the security of individually identifiable health information, as such term is defined under the HIPAA regulations. Some of our businesses collect, maintain, and/or access individually identifiable health information and are subject to the HIPAA regulations. Our operations, depending on their location, may also be subject to state or foreign regulations affecting personal data protection and the manner in which information services or products are provided. Significant criminal and civil penalties may be imposed for violation of HIPAA standards and other such laws. We have a HIPAA compliance program to facilitate our ongoing effort to comply with the HIPAA regulations.

Enacted in 2009, the American Recovery and Reinvestment Act (“ARRA”) strengthens federal privacy and security provisions to protect individually identifiable health information. A section of the ARRA known as the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”) strengthened certain aspects of the HIPAA privacy and security rules, imposed new notification requirements related to health data security breaches, broadened the rights of the U.S. Department of Health and Human Services (“HHS”) to enforce HIPAA, and directed HHS to publish more specific security standards. On January 25, 2013, the Office for Civil Rights of HHS published the HIPAA omnibus final rule (“HIPAA Final Rule”), which amended certain aspects of the HIPAA privacy, security and enforcement rules pursuant to the HITECH Act, extending certain HIPAA obligations to business associates and their subcontractors. Certain components of our business act as “business associates” within the meaning of HIPAA and are subject to these additional obligations under the HIPAA Final Rules.

Some of our businesses collect, maintain, and/or access other sensitive personal information that is subject to federal and state laws protecting such information, in addition to the requirements of HIPAA, the HITECH
Act and the regulations implemented thereunder. Security and disclosure of personal information is also highly regulated in many other countries in which we operate, and such regulations continue to evolve. Additionally, we need to comply with applicable privacy and security requirements of countries throughout the world in which we maintain operations, including but not limited to those in the European Union.

There can be no assurances that compliance with these requirements will not impose new costs on our business. …

We are required to comply with increasingly complex and changing data privacy regulations both in the United States and beyond that regulate the collection, use and transfer of personal data, including particularly the transfer of personal data between or among countries. Many of these foreign data privacy regulations are more stringent than those in the United States. We may also face audits or investigations by one or more domestic or foreign government agencies relating to our compliance with these regulations. An adverse outcome under any such investigation or audit could subject us to fines or other penalties. That or other circumstances related to our collection, use and transfer of personal data could cause a loss of reputation in the market and/or adversely affect our business and financial position.

Retail sector

We rely extensively on computer systems to implement our integrated retail strategy, process transactions, summarize results and otherwise manage our business. Disruptions in these systems could harm our ability to run our business.

Given the significance of our online and mobile capabilities, our collection and use of data to create personalized experiences, and the number of individual transactions we have each year, including in our stores, it is critical that we maintain uninterrupted operation of our computer and communications hardware and software systems, some of which are based on end-of-life or legacy technology, operate with minimal or no vendor support and are otherwise difficult to maintain. Our systems are subject to damage or interruption from power outages, computer and telecommunications failures, computer viruses, security breaches, catastrophic events such as fires, tornadoes and hurricanes, and usage errors by our employees. Operating legacy systems subjects us to inherent costs and risks associated with maintaining, upgrading and replacing these systems and retaining sufficiently skilled personnel to maintain and operate the systems, demands on management time, and other risks and costs. Any material interruption in our computer operations may have a material adverse effect on our business or results of operations, including on our [branded] program and participation.
in or engagement with that program. We are pursuing initiatives to transform our information technology processes and systems. These initiatives are highly complex and include replacing legacy systems, upgrading existing systems, and acquiring new systems and hardware with updated functionality. The risk of disruption is increased in periods when such complex and significant systems changes are undertaken.

If we do not maintain the security of our member and customer, associate or company information, we could damage our reputation, incur substantial additional costs and become subject to litigation.

Cyber-security risks such as malicious software and attempts to gain unauthorized access to data are rapidly evolving. Techniques or software used to gain unauthorized access, and/or disable, degrade or harm our systems may be difficult to detect or scope for prolonged periods of time, and we may be unable to anticipate these techniques or put in place protective or preventive measures. These attempts to gain unauthorized access could lead to disruptions in our systems, unauthorized release of confidential or otherwise protected information or corruption of data. If individuals are successful in infiltrating, breaking into, disrupting, damaging or otherwise stealing from the computer systems of the Company or its third-party providers we may have to make a significant investment to fix or replace them, we may suffer interruptions in our operations in the interim, we may face costly litigation, government investigations, government enforcement actions, fines and/or lawsuits, the ability for our members to earn or redeem points in our [branded] program may be impacted or halted, and our reputation with our members and customers may be significantly harmed. There is no guarantee that the procedures that we have implemented to protect against unauthorized access to secured data are adequate to safeguard against all data security breaches. A data security breach or any failure by us to comply with applicable privacy and information security laws and regulations could result in a loss of customer or member confidence and negatively impact our business, including our [branded] program, and our results of operations. As publicly announced ..., [company]’s ... store payment data system [was] criminally breached [so] that debit and credit card numbers were potentially compromised. The Company is defending a class-action lawsuit ... alleging violations relating to, and harm resulting from this incident.

We are subject to payment-related risks that could increase our operating costs, expose us to fraud or theft, subject us to potential liability and potentially disrupt our business operations.

As a retailer who accepts payments using a variety of methods, including credit and debit cards, PayPal, and gift cards, the Company is subject to rules, regulations, contractual obligations and compliance requirements, including payment network rules and operating guidelines, data security standards and certification requirements, and rules governing electronic funds transfers.
The regulatory environment related to information security and privacy is increasingly rigorous, with new and constantly changing requirements applicable to our business, and compliance with those requirements could result in additional costs or accelerate these costs. For certain payment methods, including credit and debit cards, we pay interchange and other fees, which could increase over time and raise our operating costs. We rely on third parties to provide payment processing services, including the processing of credit cards, debit cards, and other forms of electronic payment. If these companies become unable to provide these services to us, or if their systems are compromised, it could disrupt our business.

The payment methods that we offer also subject us to potential fraud and theft by persons who seek to obtain unauthorized access to or exploit any weaknesses that may exist in the payment systems. The payment card industry established October 1, 2015 as the date on which it will shift liability for certain transactions to retailers who are not able to accept EMV card transactions. The Company did not implement the EMV technology and receive certification prior to October 1, 2015, and accordingly may be liable for costs incurred by payment card issuing banks and other third parties as a result of fraudulent use of credit card information improperly obtained from information captured by us until such time as the technology has been implemented and certified. The Company presently expects to complete the implementation and receive certification in its second quarter 2016.