DORSEY™
always ahead

SEC Guidance on Cybersecurity Disclosure and Policies

Cybersecurity Risk Factors

Cam Hoang
Gary Tygesson
Bob Cattanach

June 5, 2018

Cybersecurity Risk Factors: Examples

SEC Guidance on Risk Factors	Examples in Form 10-K, Item 1A
• Prior incidents, including severity and frequency	"In 2017, we were the target of a cybersecurity attack that involved the theft of certain personally identifiable information of U.S., Canadian and U.K. consumers. As a result of an ongoing analysis of data stolen in the 2017 cybersecurity incident, the Company recently announced that it was able to identify approximately 2.4 million U.S. consumers whose name and partial driver's license information were stolen, but who were not in the affected population of approximately 145.5 million consumers previously identified by the Company in 2017. The Company is in the process of notifying these additional consumers. It is possible that further analysis will identify additional consumers affected or additional types of data accessed, which could result in additional notifications and negative publicity." *Equifax Inc. Form 10-K, Item 1A, 2018*

Cybersecurity Risk Factors: Examples

SEC Guidance on Risk Factors	Examples in Form 10-K, Item 1A
• Probability and potential magnitude of future incidents	"The company's products, services and systems may be used in critical company, customer or third-party operations, or involve the storage, processing and transmission of sensitive data, including valuable intellectual property, other proprietary or confidential data, regulated data, and personal information of employees, customers and others. Successful breaches, employee malfeasance, or human or technological error could result in, for example, unauthorized access to, disclosure, modification, misuse, loss, or destruction of company, customer, or other third party data or systems; theft of sensitive, regulated, or confidential data including personal information and intellectual property; the loss of access to critical data or systems through ransomware, destructive attacks or other means; and business delays, service or system disruptions or denials of service." *International Business Machines Corp. Form 10-K, Item 1A, 2018*

Cybersecurity Risk Factors: Examples

SEC Guidance on Risk Factors	Examples in Form 10-K, Item 1A
• Aspects of business and operations that give rise to material risks, including industry-specific, third-party and service provider risks • Adequacy of preventative actions, including limits on the company's ability to prevent or mitigate certain risks	"In order to provide our services, we process and store sensitive business information and personal information about our merchants, merchants' customers, vendors, partners, and other parties. This information may include credit and debit card numbers, bank account numbers, names and addresses, and other types of personal information or sensitive business information. Some of this information is also processed and stored by our merchants, third-party service providers to whom we outsource certain functions, and other agents (which we refer to collectively as our "associated third parties"). […] Our computer systems are subject to penetration and our data protection measures may not prevent unauthorized access…. Threats to our systems and our associated third parties' systems can derive from human error, fraud, or malice on the part of employees or third parties, or may result from accidental technological failure." *GH Capital Inc. Form 10-K, Item 1A, 2018*

Cybersecurity Risk Factors: Examples

SEC Guidance on Risk Factors	Examples in Form 10-K, Item 1A
• Costs associated with protections, including insurance coverage	If we or third parties with which we do business were to fall victim to successful cyber-attacks or experience other cybersecurity incidents, including the loss of individually identifiable customer or other sensitive data, we may incur substantial costs and suffer other negative consequences, which may include…increased cybersecurity and other insurance premiums; *Burlington Store, Inc. Form 10-K, Item 1A, 2018* We have cybersecurity insurance related to a breach event covering expenses for notification, credit monitoring, investigation, crisis management, public relations and legal advice….. We also maintain property and casualty insurance that may cover restoration of data, certain physical damage or third-party injuries caused by potential cybersecurity incidents. However, damage and claims arising from such incidents may not be covered or may exceed the amount of any insurance available. *Otter Tail Corp Form 10-K, Item 1A, 2018*

Cybersecurity Risk Factors: Examples

SEC Guidance on Risk Factors	Examples in Form 10-K, Item 1A
• Potential for reputational harm	"Reputation. Our reputation is an important corporate asset. An operating incident, significant cybersecurity disruption, or other adverse event such as those described in this Item 1A.may have a negative impact on our reputation, which in turn could make it more difficult for us to compete successfully for new opportunities, obtain necessary regulatory approvals, or could reduce consumer demand for our branded products." *Exxon Mobile 2018 Form 10-K, Item 1A Risk Factors.*

Cybersecurity Risk Factors: Examples

SEC Guidance on Risk Factors	Examples in Form 10-K, Item 1A
• Costs of compliance with laws and regulations	The Company is subject to regulatory environment changes regarding privacy and data protection and could have a material impact on our results of operations. The growth and expansion of the company into a variety of new fields may potentially involve new regulatory issues/requirements such as the EU General Data Protection Regulation (GDPR) or the New York Department of Financial Services (NYDFS) Cybersecurity Regulation. The potential costs of compliance with or imposed by new/existing regulations and policies that are applicable to us may affect the use of our products and services and could have a material adverse impact on our results of operations. *Berkshire Hills Bancorp Inc. Form 10-K, Item 1A, 2018*

Cybersecurity Risk Factors: Examples

SEC Guidance on Risk Factors	Examples in Form 10-K, Item 1A
• Costs of litigation, investigations and remediation	These cybersecurity incidents have increased in number and severity and it is expected that these trends will continue. Should the Company be affected by such an incident, we may incur substantial costs and suffer other negative consequences, which may include: • remediation costs, such as liability for stolen assets or information, repairs of system damage, and incentives to customers or business partners in an effort to maintain relationships after an attack; […] • litigation and legal risks, including regulatory actions by state and federal regulators *Siebert Financial Corp. Form 10-K, Item 1A, 2018*