Vermont ski area reports Hannaford-like theft of payment card data – Okemo says card info was stolen as cards were swiped, as in breach at grocery chain

In a security breach that sounds similar to the one disclosed by Hannaford Bros. Co. last month, the Okemo Mountain Resort ski area in Vermont announced this week that data from more than 46,000 credit and debit card transactions may have been compromised during a system intrusion over a 16-day period in February... Bonnie MacPherson, a spokeswoman for Okemo, said today that at least some of the data appears to have been stolen as the recent payment card transactions were being authorized. "We can tell you that this was a real-time theft," McPherson said. "The information was being taken as the cards were being swiped."

We are all familiar with these types of headlines, yet how many resorts have really considered the implications of cyber theft...?

Today, with network-centric operations the norm in most industries – retail, medical, financial, legal, hospitality – some of a company’s most critical assets are intangible: electronically stored information. In fact, a significant portion of any company’s value is tied up in its electronic information assets – as much as 70 percent in some cases according to Gartner, Inc., a preeminent technology research and advisory firm. Network security and privacy risk (aka “cyber risk”) insurance was developed to protect a company’s intangible assets, and its reputation. It addresses the unique risk exposures associated with the electronic processes, interactions and digital assets related to network-dependent business activities. Almost every business, regardless of the product or service it provides, has some degree of cyber risk exposure, such as unauthorized access to data (from internal or external sources), computer viruses, denial-of-service attacks and poor network management. The ski industry, as well as other sports and recreation businesses, is no exception. Because identity theft is one of the fastest growing crimes worldwide, various privacy regulations (HIPAA, GLBA, FACTA, State Notice Laws) require that companies protect sensitive customer and employee data no matter where it resides: on the network; on standalone systems such as billing, medical, and marketing databases; on remote devices, such as laptops; on outsourced vendor networks; and on paper. So in addition to the risk of lost business, companies now face a larger risk to their reputation and the potential for class-action lawsuits. Recently passed regulations and industry standards, such as PCI DSS (Payment Card Industry Data Security Standards), add to a company’s overall risk in the form of fines and penalties for noncompliance.
Failure to take the necessary measures to secure information, and to mitigate potential loss if measures taken should fail, may result in significant financial costs for a business. When a cyber risk event occurs, the consequences can be financially crippling to a company with the emergence of class action lawsuits, huge forensic and mitigation costs, possible identity theft damage litigation and the potential loss of reputation and customers. The most damaging financial impact of these risks is most likely to come in the form of litigation. Several companies that have reported a major security breach are now facing privacy-related class action lawsuits that may require years of litigation and cost millions of dollars. But even when there is no lawsuit, there are extraordinary expenses involved.

46 states now require companies, by law, to notify every person whose personal identity information was compromised—which can take weeks and a huge expenditure of manpower. Systems need to be shut down, business is interrupted, a public relations and damage control campaign needs to be launched, specialty investigation and forensic experts hired, and if it involved credit card information, cardholders, issuing banks and credit bureaus need to be notified. Information assets and records need to be restored. Consumer banks might seek reimbursement for credit card-related losses. Additionally, corporate officers can be held personally liable if they fail to provide adequate network security or act diligently to prevent breaches from occurring. Cyber risk exposure is divided into two degrees of risk: direct risks and indirect risks. Direct risks include the actual theft of customer information, trade secrets or money, damage to critical electronic data, and productivity losses that are real but may be difficult to quantify. Indirect risks are potentially more costly than direct risks and include loss of customers, damage to brand and loss of reputation.

A comprehensive cyber risk insurance policy covers breaches caused by both internal and external factors, including employee errors in handling sensitive data. Cyber risk insurance is usually offered in modular form, so you can select the type and amount of coverage needed for your type of business. Available coverage includes:

- Business income loss including extra expense
- Data restoration expenses
- Public relations and consumer notification expenses
- Cyber extortion expenses
- Litigation and regulatory defense expenses

While network security and privacy is still a relatively new area of coverage, the number of insurers offering this coverage has increased considerably in the past few years. There is now adequate capacity available for even the largest companies to obtain good protection against the financial and reputational crisis that could occur in the wake of a data breach event.

To learn more about our exclusive digital risk solutions, contact your Wells Fargo Special Risks representative.

For more information, contact Helen Richards,
800-528-7730 • helen.richards@wellsfargo.com

This publication is intended to be a general discussion of the matters contained herein and the information should not be used in making a decision concerning the subject matter without consulting with your attorney, accountant or insurance professional. Wells Fargo Special Risks, Inc. assumes no responsibility whatsoever in accordance with its use.

Prepared by the Sports & Recreation Division of Wells Fargo Special Risks, Inc.