IN A WORLD OF BIG DATA – BREACHES CAN COST BIG DOLLARS

Cybersecurity & Privacy Alert
February 1, 2019

Practices & Industries

Cybersecurity & Privacy

The Dallas-based luxury department store chain, Neiman Marcus Group, Inc. (the Company), recently settled an investigation of its 2013 data breach with 43 states and the District of Columbia for $1.5 million. The data breach affected private customer data attached to roughly 370,000 credit cards – at least 9,200 of which were fraudulently used by hackers to complete unauthorized transactions or sold to the highest bidder on the dark web.

Attorney Generals (the "AGs") from Maryland, Illinois, and Connecticut led the investigation on behalf of all affected states and as a result of the settlement, the AGs in all of the states involved agreed not to pursue individual claims against the Company in exchange for its implementation of stronger data security measures to prevent future attacks.

By way of background, early in the investigation (January 22, 2014) the Company acknowledged that its point-of-sale data was breached and that compromised debit and credit transactions date all the way back to July of 2013. The Company's President and CEO stated that a network malware attack designed to collect payment card data was identified by data forensics investigators. The attack compromised data held across 77 stores and took place over several months. The data included names, dates of birth, payment history, and social security numbers.

After five years of investigation and settlement negotiations, the Company agreed to a $1.5 million settlement, but that is not the only expense of this breach. During the investigation into the breach, the Company likely spent hundreds of thousands of dollars on forensic, professional and legal fees. And this dollar amount does not begin to contemplate potential negative reputational issues. Additionally, as part of the settlement, the Company must entirely revamp its data security policies and practices.

Specifically, the Company must enhance its security protocols to comply with payment card industry data security standard requirements, including the following measures: (1) maintain a system log to routinely monitor all network activity; (2) maintain agreements with payment card industry forensic investigators, operating separately to allow for speedy remediation of any hacks or breaches; (3) frequently update software used to maintain and protect consumer data; (4) implement industry-accepted payment security technologies; and (5) use of encryption and

tokenization techniques to obscure payment card and consumer data. The settlement also requires the Company to obtain an information technology security assessment from a third party and detail any areas needing improvement.

What Does This Mean For Your Company?

Perhaps the biggest takeaway from this situation is that state and federal government actors and regulators are taking data breaches, no matter the size, extremely seriously, and so should your company. Maryland Attorney General Brian E. Frosh implored that "businesses that collect and hold consumers' payment card data have a responsibility to make sure that data is protected from hackers." To uphold your obligation as a business or employer handling sensitive or personal data, here are a few things you can do to protect your company's interests, protect company data and the data your company holds on behalf of others:

- **Conduct a security audit to identify vulnerabilities.**
- **Conduct regular/routine staff training to mitigate risk of entry points based on human error.**
- **Require multi-factor authentication and alpha-numeric and symbol passwords.** Complex passwords that change often may drastically reduce this vulnerability.
- **Data encryption.**
- **Back-up data.** Security is paramount, but in the event of a breach, hackers can often destroy data or prevent your access to your own data. If your data is not backed up, it could be gone forever.
- **Have clear and simple security policies in place for employees.** For example, require all notebook computers and mobile devices connected to the business network to have security software.
- **Protect your mobile work force.** As more employees are working away from the office – and away from the protection of your network security – it is important to ensure wireless technology is as secure as possible.
- **Have a multi-pronged data solution.** Viruses and malware are not the only threat. Hackers and their attacks are more sophisticated than ever, and having multiple layers of security technology on all devices (meaning every desktop, mobile device, filer server, mail server, and network end point) to comprehensively secure your data, is absolutely crucial. Multiple layers of security can isolate attacks from affecting all of your data and/or alert you to a problem so your IT team can take appropriate action.

Securing your business's data is not easy and takes expertise. At the time of this breach, nearly a dozen other major retailers, banks, and public corporations experienced similar attacks resulting in immense remedial efforts and costs, many of which could have been prevented. One of the most important things you can do to avoid becoming the next victim is to train your employees in data security best practices and ensure that your employees understand the critical role they each play in securing company data.

For questions regarding your current data security measures or regulatory compliance, contact one of Hodgson Russ's Cybersecurity & Data Privacy Practice attorneys.

If you received this alert from a third party or from visiting our website, and would like to be added to our Cybersecurity & Data Privacy Practice mailing list or any of our other mailing lists going forward, please visit https://forms.hodgsonruss.net/sign-up-for-email-and-other-communications..html.