CLIENT ALERT: Recent Data Security Breaches Highlight the Importance of Compliance with the Massachusetts Data Security Law

Since the Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 C.M.R. 17.00, *et seq.* (the "Regulations"), took effect on March 1, 2010, there have been several notable breaches that have tested their reach and have begun to provide insight into how the Massachusetts Attorney General's Office will enforce the Regulations. The Regulations mandate that businesses develop, implement, maintain and monitor a comprehensive written information security system to protect personal information. Personal information includes a resident's first name and last name or first initial and last name in combination with any one or more of the following: (a) social security number; (b) driver's license number or Massachusetts identification card number; and/or (c) financial account number, or credit or debit card number.

Breach at Division of Unemployment Assistance

In May 2011, the Massachusetts Executive Office of Labor and Workforce Development announced that approximately 225,000 people in Massachusetts could become victims of identity theft due to a data breach in the Commonwealth's unemployment system. The potential victims include those who are currently receiving jobless benefits and those who have used a state career center computer in the past month. Also, approximately 1,200 employers may be affected if they manually entered information into the Division of Unemployment Assistance's ("DUA") system. The Qakbot virus infected approximately 1,500 computers when someone visited a website with a malicious code. It is believed to have retrieved names, addresses, Social Security numbers, and other data and transmitted it to hackers, although the investigation is still ongoing as to what and how much information was actually stolen. Joanne Goldstein, the Secretary of Labor and Workforce Development, has recommended that possible victims act immediately to place a credit freeze or security alert on their credit reports. The Commonwealth is

also sending notification letters to all possible victims.

As a state agency, the DUA is subject to the Massachusetts Data Security Regulations, 201 CMR 17.00 *et seq.* through an Executive Order signed by Governor Deval Patrick in September 2008. This breach at the DUA is believed to have occurred on April 20, 2011. Although the Regulations require businesses to report a breach "as soon as practicable and without unreasonable delay," there is an exception when the breach is subject to a criminal investigation. It is unclear whether the DUA's delay in reporting this breach to suspected victims was due to an ongoing investigation, which involves state and federal authorities that are tracking the suspected hackers.

Sony Network Entertainment Announces Breach

Also, in April 2011, Sony Network Entertainment reported a massive security breach by hackers that may have acquired the personal information of 77 million users of its PlayStation Network and Qriocity online services. Sony announced that the compromised data may include users' names, addresses, countries, e-mail addresses, birth dates, PlayStation Network/Qriocity password and login, and handle/PSN online ID. Other data that may have been compromised includes profile data and purchase history, including credit card numbers. Massachusetts Attorney General Martha Coakley contacted Sony, notifying it by letter that it must provide proper legal notice to all affected Massachusetts consumers in accordance with Chapter 93H of the Massachusetts General Laws.

Briar Group, LLC Settles Data Security Breach Lawsuit

On March 28, 2011, Attorney General Coakley's Office entered into a settlement agreement with the Briar Group, LLC, a restaurant company that owns and operates several Boston restaurants, including The Lenox, MJ O'Connor's, Ned Devine's, The Green Briar, and The Harp. The Attorney General's Office filed a lawsuit against the Briar Group in Suffolk Superior Court after the group experienced a data breach in April 2009. A malcode was installed on the Briar Group's computers, which allowed hackers to access customers' credit and debit card information. The Briar Group reported the breach to the Attorney General's Office.

The complaint alleged that the Briar Group failed to change default usernames and passwords, permitted employees to share common usernames and passwords,

failed to properly secure its remote access utilities and wireless network, and continued accepting customers' credit and debit card information after the breach. The Attorney General's Office and the Briar Group disagreed over whether the Briar Group failed to promptly address the breach. The malcode was on the Briar Group's system from April until December 2009. The complaint alleged that the Briar Group waited too long to take action after it learned of the breach; delayed engaging an outside forensics investigation team; and, that there was too much time between the start of the forensic investigation and the removal of the malcode.

In the settlement agreement, the Briar Group agreed to pay $110,000 in civil penalties, comply with the Regulations, comply with the Payment Card Industry Data Security Standards, and establish an enhanced computer network security system. Also, all Briar Group restaurants must develop a security password management system, implement data security measures that comply with the Payment Card Industry Data Security Standards, and implement and maintain a Written Information Security Program ("WISP"). It should be noted that this breach occurred before the Regulations took effect.

These data security breaches highlight the importance for companies of implementing, maintaining, and enforcing a WISP. Also, it is essential that companies take prompt action in addressing a suspected breach. If a company believes that its computer system has been hacked, it is essential that it terminate the identified and/or suspected vulnerabilities to its system. The Briar Group settlement demonstrates that the Attorney General's Office will aggressively enforce the Regulations and will penalize companies for delayed action.

Employers are advised to consult with their MBJ attorney with any questions about compliance with the data security law, or any other labor and employment related issues.

Rachel E. Muñoz is an attorney with Morgan, Brown & Joy, LLP. Rachel may be reached at (617) 523-6666 or at rmunoz@morganbrown.com. *Morgan, Brown & Joy, LLP focuses exclusively on representing employers in employment and labor matters.*

This alert was prepared on May 18, 2011.

opinion on any specific facts or circumstances by Morgan, Brown & Joy, LLP and its attorneys. This newsletter is intended for general information purposes only and you should consult an attorney concerning any specific legal questions you may have.Customize the Author Byline?
byline-default