Employment Law Report

Spring 2014

Is your business prepared for a data breach?

Small businesses face cyber threats -- and regulatory security mandates.

By Eric R. Harlan and Matthew A. S. Esworthy

Late last month the University of Maryland announced that it suffered a cyber attack that compromised the personal information of over 300,000 faculty, staff, students, and alumni. Earlier this month, Johns Hopkins University officials revealed that personal information belonging to over 1300 current and former students had been stolen from a university web server. These attacks came on the heels of a massive Christmastime data breach at Target in which cyber thieves stole credit card information of over 100 million consumers.

Small and medium-sized employers that do not maintain voluminous client or consumer personal information may not consider themselves worthy hacker targets, and may believe they're safe from such a cyber attack. They should think again. Hackers and identity thieves want personal information—and the personal information of a company's employees is just as good as that of a retailer's customer or a university's alumni. And if a business is not prepared to handle a data breach, it risks claims from its employees.

The Maryland Personal Information Protection Act targets employers throughout the state.

Currently, 46 states, including Maryland, have enacted laws concerning the protection of personal information. The Maryland Personal Information Protection Act ("PIPA") mandates that all businesses "implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information" maintained by the business. PIPA defines "personal information" as a person's first name or initial and last name, in combination with any of the following: (i) social security number; (ii) driver's license number; (iii) financial account/credit card number and pass code; and (iv) taxpayer identification number. Personal information does not include information that is lawfully made available to the public in government records, or information provided in accordance with HIPPA.

Although codified as a "Consumer Protection Provision" of Maryland's

Continued on Reverse>>

SHAPIRO SHER GUINOT & SANDLER

About the Firm

In 2013, for the third consecutive year, Shapiro Sher Guinot & Sandler was named the top medium-size law firm in Maryland for Business & Transactions by Super Lawyers, a division of Thomson Reuters. Founded by sports lawyer Ronald M. Shapiro in 1972, the firm represents clients in numerous practice areas, including employment law, litigation, corporate, real estate, tax, and banking.

Shapiro Sher Guinot & Sandler's **Employment Law Group** is co-chaired by **Eric R. Harlan** and **Renée Lane-Kunz**. They are prepared to assist organizations with a wide spectrum of employment law matters, including recruiting and hiring practices, employee handbooks, discrimination matters, executive compensation, wrongful termination claims, and issues involving Title VII of the Civil Rights Act, The Family and Medical Leave Act, and The Americans with Disabilities Act. The Employment Law Group also assists with employment, severance, non-disclosure and non-compete agreements, among other matters.

Renée Lane-Kunz offers ongoing employment counsel to small and mid-sized companies as well as schools and institutions. She works closely with clients to help them anticipate and avoid litigation and regulatory complications. From handbooks to employment agreements, to general HR policies, she is ready to provide employers the tools they need in today's legal environment. As she brings to her practice extensive HR management experience in the hospitality industry, she fully appreciates the concerns of business owners.

Eric R. Harlan is a trial lawyer dedicated to the vigorous representation of clients in litigation. He has achieved favorable results in employment-related matters including claims involving violations of federal and state anti-discrimination laws, actions to enforce non-compete and non-solicitation agreements, wrongful discharge, and wage-and-hour litigation.

Commercial Law article, PIPA is not limited to protecting consumers; it applies with equal force to the personal information of a business's Maryland employees and job applicants. That means employers should consider how they are protecting job applicant files and employee personal data. Hackers are not the only threat; current and former staff may also compromise such data.

In the event of a security systems breach—which can range from a sophisticated cyber attack to a misplaced laptop computer—the law requires the business first to investigate the breach. If the investigation determines that an individual's personal information has been misused, or that misuse is "reasonably likely to occur," a business must then notify the affected individuals of the breach, and provide them with information to help them address potential identity theft. (The law permits delays in notification (i) at the request of law enforcement agencies so as not to impede a criminal investigation, or (ii) to determine the scope of the breach, identify the affected individuals, and/or restore the integrity of the breached system.)

Maryland's "Wall of Shame" and PIPA's notification requirements

A unique feature of Maryland's law is that not only must a business notify the individual whose information was improperly accessed, but it must also notify the Attorney General of the security systems breach *before* notifying the individual. Notably, these notice letters are publicly posted on the Attorney General's website, which some commentators have referred to as the "wall of shame." Failure to comply with this and any other provision of PIPA is deemed an unfair or deceptive trade practice, and subject to the enforcement and penalty provisions of Maryland's Consumer Protection Act.

Ultimately, in the event of a data breach, an employer could face liability for damages from failing to implement reasonable security procedures and practices in the first instance, and then face additional penalties if it fails to comply with the required investigatory and notice requirements.

But PIPA may just be the tip of the compliance iceberg, as it speaks only to personal information of Maryland residents. To the extent a Maryland business maintains personal information of employees or others who reside in different states, or conducts business in other states, those jurisdictions' laws may apply. For example, Pennsylvania's "Breach of Personal Information Notification Act" applies to all businesses, not just those organized under Pennsylvania law, that maintain personal information of residents of its Commonwealth. Each state's law will have its own specific requirements, which creates a myriad of potential compliance pitfalls.

The University of Maryland and Target data breaches should serve as a reminder to employers—whatever their size—not only to assess the integrity of their information security systems, but to also develop a plan of action for responding to a potential data breach.

For more information, please contact Eric R. Harlan at erh@shapirosher.com or Matthew A. S. Esworthy at mase@shapirosher.com. Both partners can also be reached at 410.385.0202.

DOL to Update Federal Overtime Rules

Business owners stay tuned: President Barack Obama has ordered the U.S. Department of Labor to revise federal rules on overtime pay to make more employees eligible for time-and-a-half. This is the President's latest executive action to reduce "income inequality," and many are calling it his most ambitious to date.

Currently, the cap on mandated overtime pay for salaried workers is $455 a week, or roughly $24,000 a year. The President has directed the Labor Department to increase the salary threshold and change the definition of a "supervisor," so that lower-level employees with only minor supervisory duty will still be eligible for overtime pay when they work more than 40 hours a week.

Though the President's directive bypasses congressional scrutiny, it is highly unlikely that any changes to overtime-related regulations will be implemented this year. The first step is for the Labor Department to draw up a plan to increase the number of workers eligible for overtime pay, followed by a period of public comment. As the mid-term elections approach, expect talk of changes to overtime pay to continue and anticipate that changes designed to increase the number of workers eligible for overtime are forthcoming.