MIAMI-DADE THURSDAY, JUNE 17, 2021

OFFICIAL COURT NEWSPAPER OF SOUTH FLORIDA
DailyBusinessReview.com
An ALM Publication VOL. 95, NO. 251 $2.00
DAILY BUSINESS REVIEW

PRACTICE FOCUS / CYBERSECURITY

Addressing Pandemic-Related Cyberattacks and the Legal Implications for Employers

Commentary by
Barron F. Dickinson

Due to the majority of the general workforce's shift to remote work following the onset of the COVID-19 pandemic, the frequency of cyberattacks has dramatically increased by 600%.


Dickinson

According to the 2020 Cost of a Data Breach Report issued by IBM, the average total cost of a data breach is $3.86 million, and the average amount of time for a company to identify and contain a data breach is 280 days. In addition, 76% of the participants who were surveyed by IBM reported that remote work would likely increase the time necessary to identify and contain a data breach.

Prior to the pandemic, a 2017 study conducted by Nationwide Insurance estimated that 58% of U.S. businesses have experienced a cyberattack. More than 20% of those victims reported spending at least $50,000 and needing more than six months to recover. Notwithstanding, less than half of the businesses surveyed reported having established security policies and practices.

DOL ISSUES GUIDELINES

This rise in cyberattacks on companies in the United States has resulted in the U.S. Department of Labor's (DOL) novel issuance of guidance for plan sponsors, plan fiduciaries, record keepers and plan participants on best practices for maintaining cybersecurity. Employers' concerns regarding the detrimental impact that a data breach could have on their business and operations are well founded, including the extent of their liability where employees' and consumers' confidential personal information is stolen by hackers.

For example, in March of this year, hackers stole approximately 26,000 files from the Broward County School District, some of which contained confidential student and employee information, and demanded a ransom of $40 million in exchange for returning the files. The school district refused to meet the hackers' demands and consequently, the hackers published the files on the internet.

EMPLOYERS' POTENTIAL FOR LIABILITY

The extent of an employer's liability following a data breach that results in the disclosure of employees' confidential information is a developing area of the law in Florida and the Eleventh Circuit. The Eleventh Circuit has held that an elevated risk of identity theft and evidence of a data breach alone is insufficient to establish an injury-in-fact, which is necessary to confer standing under Article III of the U.S. Constitution. Instead, a plaintiff must allege that the data breach placed him or her at a substantial risk of future identify theft or that the identity theft was certainly impending.

BOARD OF CONTRIBUTORS

Courts outside the Eleventh Circuit have also dismissed claims brought by employees against the employer following the theft of their personal confidential information on the basis that the injuries claimed by the employees were speculative in nature, did not reflect any actual harm, and the employer did not owe a duty to its employees to prevent their confidential information from being stolen by third parties in a data breach. Notwithstanding, plaintiffs in Florida have enjoyed a degree of success recently in surviving the motion to dismiss stage when alleging data breach claims premised on a theory of negligence.

EMPLOYERS' NOTIFICATION OBLIGATIONS

Outside the litigation realm, in addition to notifying law enforcement, employers also likely have an obligation to notify their employees of a data breach that resulted in the theft of their personal information under Florida's Information Protection Act of 2014 (FIPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Under FIPA, following a data breach that results in the unauthorized access of an individual's personal information, an employer is required to notify each individual whose information was accessed of such breach within 30 days. If a data breach affects more than 500 individuals, an employer must also notify the Florida Department of Legal Affairs within this same timeframe. If a data breach affects more than 1,000 individuals, an employer must also notify all consumer reporting agencies as well.

Similarly, employers who meet the definition of a "covered entity" under HIPAA are required to notify individuals whose protected health information has been improperly accessed of a breach within 60 days of discovering the breach. In addition, if the breach results in the unauthorized disclosure of more than 500 individuals' information, an employer is required to notify the media and the Secretary of Health and Human Services within this same timeframe.

Fortunately for employers, neither FIPA nor HIPAA provides a plaintiff with a private right of action to enforce these statutes. However, employers may still face investigations and stiff fines from the State of Florida and the federal government should they fail to satisfy their obligations under FIPA and HIPAA.

TAKING PROACTIVE MEASURES

Employers should always take proactive measures to protect employees' personal and confidential information. In particular, employers should install encryption and wiping software on all employee-issued devices, require complex passwords, and establish mandatory and recurring cybersecurity training to educate employees on the latest cybersecurity attack methods and best practices regarding data protection. Employers may also want to consider adopting and enforcing cybersecurity policies in their handbook as more than 50% of all security incidents are caused by employees. In drafting such policies, employers should also consider creating a cybersecurity incident response plan that includes the formation of a dedicated response team.

Lastly, many insurance companies are now offering what is called "data breach and cyber liability insurance." Employers may want to consider consulting with their current coverage providers or the general insurance marketplace to inquire as to terms and provisions of such coverage, as well as providers' experiences in defending data breach claims brought by third parties.

Barron F. Dickinson is an attorney with the Miami-based law firm Allen Norton & Blue, a statewide firm devoted exclusively to the practice of labor and employment law. Contact him at bdickinson@anblaw.com.