Bodman PLC | Workplace Law Practice | www.bodmanlaw.com January 24, 2019

EMPLOYERS RESPONSIBLE FOR BOTH CUSTOMER AND EMPLOYEE INFORMATION IN DATA BREACH CASES

By: Donald H. Scharg, Member, Workplace Law Practice

Reports of computer hacks and data breaches are becoming too commonplace. Large companies are often the victim and their customer information the target. But, what happens when an employer is a subject of a data breach and its employee records are hacked? The recent Pennsylvania Supreme Court decision in Dittman v. UPMC (Pa. Nov. 21, 2018) highlights employers' obligation to protect both customer and employee information stored on their computers.

Like many employers, the University of Pittsburgh Medical Center (UPMC) collected personal and financial information from its employees. Hackers accessed UPMC's computers and stole the personal and financial information of 62,000 current and former employees. The employees alleged that the hackers used the stolen data, which consisted of information UPMC required employees to provide as a condition of their employment, to file fraudulent tax returns.

The affected employees filed a class action lawsuit seeking to recover damages against UPMC under a negligence theory. The employees alleged that UPMC had a duty to exercise reasonable care to protect their "personal and financial information within its possession or control from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties" because UPMC required employees to provide information as a condition of their employment. They also claimed that UPMC breached its duty of reasonable care to them by failing to adopt, implement, and maintain adequate security measures to safeguard the information, by failing to adequately monitor the security of the network, by failing to prevent unauthorized access to the information, and by failing to recognize in a timely manner that the information had been compromised. The employees sought money damages from their employer related to damages from fraudulently filed tax returns and "increased and imminent risk of being victims of identity theft crimes, fraud, and abuse."

Both the trial and appellate courts dismissed the case. But, the employees found a sympathetic ear from the Pennsylvania Supreme Court which agreed with the employees that "in collecting and storing Employees' data on its computer systems, UPMC owed Employees a duty to exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act."

The Court concluded that "an employer has a legal duty to exercise reasonable care to safeguard its employees' sensitive personal information stored by the employer on an internet-accessible computer system." Although UPMC argued that it was not responsible for third-party criminal conduct, the Pennsylvania Supreme Court concluded that liability can be found if UPMC "realized or should have realized the likelihood

Copyright 2019 Bodman PLC. Bodman PLC has prepared this Workplace Law Client Alert for informational purposes only. This message is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act upon this information without seeking professional counsel.

that such a situation might be created and a third person might avail himself of the opportunity to commit such a tort or crime." The case was returned to the trial court where the employees were required to prove UPMC's negligence and their damages.

Michigan has laws which address notice of data breaches, but not damages that arise from data breaches. Data breach notification obligations are triggered by the unauthorized acquisition of unencrypted personal information. In order to take advantage of the notice exception, the employer must evaluate the breach and the encryption measures that are in place and determine whether the hacker also stole the key to unlock the encrypted data.

ABOUT THE AUTHOR

DONALD H. SCHARG

Mr. Scharg has more than 30 years of experience in the areas of labor law, construction labor law, employment discrimination, and employee relations. He has represented employers in collective bargaining contract arbitrations, 312 arbitrations, wrongful discharge, and discrimination claims. Don has conducted many seminars for management on employment discrimination, sexual harassment,wrongful discharge, family leave, and other topics. He also regularly contributes articles to professional and business publications regarding employment law issues.

WORKPLACE LAW PRACTICE GROUP

AARON D. GRAVES | *Chair* 313.392.1075 agraves@bodmanlaw.com	**CHRISTOPHER P. MAZZOLI** 248.743.6066 cmazzoli@bodmanlaw.com	**DAVID B. WALTERS** 248.743.6052 dwalters@bodmanlaw.com
JOHN C. CASHEN 248.743.6077 jcashen@bodmanlaw.com	**DONALD H. SCHARG** 248.743.6024 dscharg@bodmanlaw.com	**KAREN L. PIPER** | *Of Counsel* 248.743.6025 kipper@bodmanlaw.com
STEVEN J. FISHMAN 248.743.6070 sfishman@bodmanlaw.com	**MELISSA M. TETREAU** 248.743.6078 mtetreau@bodmanlaw.com	

Copyright 2019 Bodman PLC. Bodman PLC has prepared this Workplace Law Client Alert for informational purposes only. This message is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act upon this information without seeking professional counsel.