Bond

INFORMATION MEMO
LABOR AND EMPLOYMENT LAW

APRIL 2016

Preventing Unauthorized Access to and Disclosure of Confidential Employee Information

Inherent in all employment relationships is the fact that employers are privy to all sorts of confidential information about their employees. For example, in order to do something as simple as paying an employee's wages, an employer will generally need to know the employee's social security number, and, in cases of direct wage deposit, will also need to know the employee's bank account information. Employers also often come into possession of confidential medical information in connection with employees' requests for medical leaves of absence under the Family and Medical Leave Act, or when engaging in the "interactive process" with disabled employees who have requested accommodation for their disabilities.

Because employers are necessarily privy to confidential employee information, they are also inherently at risk for unauthorized disclosure of such information to others. Especially with all of the news in recent months about consumer and employee data breaches, employers should question whether the security measures they have in place to protect private employee information are actually sufficient.

But even those employers who have generally taken appropriate security measures are not necessarily immune from potential liability and are still at risk for potential disclosure of confidential information. Take, for example, the situation where an employer, who has otherwise implemented appropriate controls to protect confidential information, is undergoing maintenance of its IT system, and during the maintenance process certain file access restrictions are temporarily disabled. That is precisely the situation that occurred in *Tank Connection, LLC v. Haight*, a case that was decided by the U.S. District Court for the District of Kansas on February 5, 2016.

The employer in *Tank Connection*, a manufacturer of above-ground storage tanks with approximately 300 employees, was like many other employers with regard to how it limited employee access to its IT systems: "Each employee's computer was password protected. Access to data on the server was controlled by user-account privileges (Microsoft Active Directory). The user accounts were set up with standard authentication practices including user name and password." The company also had certain IT directories and files that were only accessible to Tank Connection's president and network administrator because they contained confidential and proprietary information. So far, so good. But here comes the problem. When the company changed its IT servers, certain security settings were not correctly transferred from the old server to the new, and a file whose access was previously restricted to the president and network administrator was now accessible to employees. Unfortunately, this mistake was not discovered by the company until after a particular employee, who was leaving the company to work for a competitor, accessed and copied confidential information from the file just prior to leaving Tank Connection.

When the mistake was ultimately discovered, Tank Connection took legal action to recover the information from the now former employee. The company claimed that notwithstanding the mistake with the IT server, the employee accessed the information without authorization and essentially "stole" it from the company. But the court ultimately rejected this claim, reasoning: "The problem with Tank Connection's argument that [the employee] exceeded his authorized access is that it is premised upon a restriction that was supposed to be incorporated into its network settings, but which in fact was not. . . . The fact that Tank Connection inadvertently provided [this employee] with access to the folder did not restrict or limit his authority. Nor does the fact that [the employee] apparently accessed these folders for purposes contrary to Tank Connection's interests amount to evidence that he exceeded 'authorized access.'"

In other words, despite Tank Connection's intent to maintain confidentiality of the file, the inadvertent mistake that occurred with the IT server resulted in the company failing to properly protect the confidential information and exposing it to potential disclosure and misuse.

An important lesson should be learned from the *Tank Connection, LLC* case — actions speak louder than intentions with regard to maintaining confidentiality. Even an employer's best intentions to protect the confidentiality of employee information can go awry and will be rendered meaningless if the employer's actions do not actually safeguard the information at issue. To ensure that intentions match actions, employers should regularly audit their information security protocols, including all security measures in effect on their IT systems to protect confidential employee information kept in electronic form, to ensure the continued functionality of such measures and make sure that what they think is in place actually is.

To learn more, contact Jessica C. Moller at 516.267.6332 or jmoller@bsk.com.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond