PUBLICATION

Psst! Can You Keep a Secret? No, Really.

October 22, 2009

In *LVRC Holdings LLC v. Brekka* (September 15, 2009), the Ninth Circuit Court of Appeals served up a warning for employers to review their existing Confidential Information policies or risk finding themselves unable to protect their most valuable information, including trade secrets. In *Brekka*, an employee e-mailed company information to his personal e-mail account shortly before his departure. He later used that confidential information to further his own business interests. Unfortunately, because the employee was authorized to access his employer's computer, as well as the information he emailed to himself, the Court held that these otherwise disloyal acts did not violate the federal Computer Fraud and Abuse Act designed to protect employers from this very behavior. Had the employer developed and circulated a computer policy prohibiting access to company files for personal use, the Court noted, such behavior would have violated the law.

In light of this and similar holdings, employers are urged to develop and/or update their Confidential Information Policy to include, at a minimum, the following:

1. **No expectation of employee privacy.** Employees should know that whatever information they access, review, send, or create, their actions may be monitored to ensure that, among other things, confidential information is being respected.
2. **Access to and Dissemination of Confidential Information For Other Than Business Purposes Is Prohibited.** By giving employees notice that access to confidential information is provided for company business only, employers should be able to avoid the Brekka outcome.
3. **Thoughtful Document Retention Practices are Observed.** Hard copies of sensitive documents should be systemically shredded.
4. **Designate Confidential Information.** By designating what information is to be protected, employers can create varying levels of confidentiality that will often be deferred to by courts. Employers should also consider allowing access to highly confidential information only after employees have electronically received and reviewed a confidential notice prior to review of this information.
5. **Password Protection.** Once confidential information has been designated, passwords should be used (and disabled) to restrict access to "need to know" information only.

In addition to abiding by these guidelines, employers should also take the following steps to better protect confidential information:

6. **Execute Confidentiality Agreements.** Confidentiality agreements with employees who will enjoy access to confidential information may also include non-solicitation, non-compete, non-disclosure, and non-recruitment provisions to fully protect confidential information.
7. **Conduct exit interviews.** A good exit interview can provide employers with insight into which employees pose a risk to take confidential information with them upon their departure. Questions to ask include what information has been accessed recently or what information an employee has plans to take. In addition, employers should solicit the name of the departing employee's future employer, remind the employee of any confidentiality agreements that have been executed during their tenure with the company and the employee's duty to abide by same, provide a signed copy of any confidentiality agreements, have employees confirm the return of all confidential information prior to

departure, and ask employees about any information that has been deleted, downloaded, or copied prior to their departure.

8. **Preserve Computer Records.** If during the exit interview it becomes clear that the departing employee is a risk to take or divulge confidential information, a copy should be made of the departing employee's hard drive.
9. **Return All Technology Devices.** Require departing employees to return all technology devices that may contain confidential information. This includes laptops, flash drives, cell phones, PDAs, etc.
10. **Disable Access.** Make sure that all access to company systems is revoked so that employees may not access confidential information after their departure.
11. **Monitor Access.** When possible, monitor system access prior to departure. While not always feasible, this may prove a useful way to ensure that no confidential information is taken or accessed unnecessarily.
12. **Enforce Consistently.** Failure to do so may result in an inability to enforce the policy against a particular employee.
13. **Respond Quickly.** If you suspect that confidential information was improperly accessed, respond quickly. In most cases, an employer must show that they took reasonable precautions to protect confidential information. The longer that an employer waits to protect confidential information, the less likely its actions are likely to be deemed reasonable in protecting it.
14. **Conduct Training on Confidential Information Policies.** This may help deter corporate theft and ensure that it is more readily noticed by supervisors.

Baker Donelson stands ready to assist you with these and other labor and employment-related challenges. Contact any one of our nearly 70 Labor & Employment attorneys located in *Birmingham, Alabama; Atlanta, Georgia; Baton Rouge, Mandeville* and *New Orleans, Louisiana; Jackson, Mississippi;* and *Chattanooga, Johnson City, Knoxville, Memphis and Nashville, Tennessee*.

Baker Donelson gives you what boutique labor and employment firms can't: a set of attorneys who are not only dedicated to the practice of labor and employment issues, but who can reach into an integrated and experienced team of professionals to assist you in every other aspect of your legal business needs. We set ourselves apart by valuing your entire company. And when it comes to your company's most valuable asset - your employees - we're committed to counseling with and advocating for you every step of the way.