BRYAN CAVE
A Broader Perspective

Alert

Labor & Employment Client Service Group

To: Our Clients and Friends

October 27, 2011

The Computer Fraud and Abuse Act (CFAA) - The Benefits of a Computer Use Policy That Restricts Employee Access

Employers that provide employees unfettered access to company computer systems may unwittingly forfeit a valuable statutory remedy against the misappropriation of electronic data. Accordingly, such employers should ensure that they have a computer use policy in place that explicitly distinguishes between authorized and unauthorized use.

The CFAA provides a federal avenue to pursue employees who have misappropriated electronic information. While the CFAA is a criminal statute, it also enables private parties to bring a civil cause of action in which they may seek "compensatory damages and injunctive relief or other equitable relief" in cases of theft or misappropriation 18 U.S.C. § 1030(g). The CFAA applies to any individual who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." *Id.* at 1030(a)(4). The CFAA also applies to any individual who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer." *Id.* at 1030(a)(5)(A). Under this second subsection, employers may bring a cause of action if they suspect an employee has misappropriated electronic data, but cannot confirm their suspicions because the employee has, for example, deleted and/or destroyed incriminating information on a company computer.

Not surprisingly, courts have focused their inquiries on the phrases "without authorization" and "exceeds authorized access." Accordingly, whether an employee will be found liable under the CFAA often turns on whether the employee was authorized to access the computer in the first place. As an employee's authorization must necessarily come from the employer, a carefully tailored computer use policy can provide employers with a powerful tool to deter and prosecute acts of theft and misappropriation. Employers that lack such policies have not faired as well in CFAA actions as courts are unwilling to hold the employee liable under the CFAA without evidence that the employee was on notice that access was unauthorized.

In crafting a computer use policy it is important to recognize that the employer-employee relationship can provide the framework for evaluating authorized versus unauthorized access to electronic data. Restricting employee access to those activities necessary to the employee's job functions should go a long way to ensure that employers are able to utilize CFAA as a remedy if problems arise. Some examples of issues to cover are:

- A signed computer use policy defining authorized versus unauthorized access;
- A description of the manner in which and purpose for which an employee may use certain information and/or databases;
- A description of circumstances under which an employee may become unauthorized and/or lose his/her authorization;
- A focus on the employee's conduct as the trigger for losing authorization; and
- Use of unique usernames and passwords for access.

The key focus for any computer use policy is *notice*. Courts will look for facts that suggest the employee was on notice that his/her use of the employer's computer was not authorized. Accordingly, employers should take care to notify employees of what data they may access, how they may access the data and to what uses they may put the data.

For additional information on this topic, please contact a member of Bryan Cave LLP's Labor and Employment Client Service Group.