PUBLICATION

How to Use the Computer Fraud and Abuse Act

January 28, 2010

The scenario

An employee has access to your company's computer though employee-specific log-in information, and he has a company email address. The employee accesses the computer and emails client lists, financial statements, and contracts from his company email to his personal email. He also uploads "scrubware," deleting all emails and files on his desktop. He quits Friday afternoon and begins working for your competitor on Monday morning.

What do you do next?

Employers can pursue traditional remedies in state court, such as breach of duty, breach of non-competition agreements (if applicable), misappropriation of trade secrets, conversion, tortious interference with business relationships, etc. But there may also be a federal remedy available.

The Computer Fraud and Abuse Act (CFAA) was enacted in 1984 and was originally designed to prosecute hackers who gained entry to computer systems via the Internet with the intent of gaining access to confidential information or causing damage though viruses and worms. Since its enactment, the CFAA has been expanded to incorporate a civil cause of action against anyone who "knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud or obtains anything of value." 18 U.S.C. § 1030(a)(4). The CFAA defines a "protected computer" as one that is used in interstate or foreign commerce, i.e. any laptop or computer connected to the Internet. However, the term "without authorization" is not defined by the statute.

What does this mean for employers?

Because practically all computers used in a business have Internet access, the CFAA is becoming a popular litigation tool for employers. Specifically, employers have filed federal litigation against former employees who obtained information from the employers' computer system and then used that information for the employees' own competitive advantage as mentioned in the scenario above. Some of these actions have been successful, while others have not. Outcomes often depend on: (1) the meaning of "without authorization," and (2) the steps taken by the employer to protect its computer systems and the information stored thereon.

Unfortunately, the United States Circuit Courts of Appeal are split as to the meaning of "without authorization," with some Circuits providing a broad interpretation, and others being more limited. For example, in *International Airport Centers, L.L.C. v. Citrin*, the Seventh Circuit recently held that an employee breached his duty of loyalty by accessing his employer's computer for an unauthorized purpose, and therefore his access to the computer was unauthorized. However, in *LVRC Holdings, LLC v. Brekka*, the Ninth Circuit recently held that the employer had given the employee "authorization" to access a company computer when it gave the employee permission to use it without limiting the employee's access and use of confidential data on the company-owned computer. With these differing definitions of "without authorization," it is important to evaluate the steps taken by the employer to limit access and use if its computer systems.

How Can Employers Increase Their Chances for Success Under the CFAA?

Until the CFAA is amended to include a definition of "without authorization" or the United States Supreme Court resolves the conflict among the Circuit Courts, there is no precise formula to increase the likelihood of a successful CFAA action. We suggest that employers consider taking the following steps:

- Review current computer policies (or formulate them if none exist) to define acceptable and unacceptable use of the employer's computer system and the information contained thereon.
- Specifically address telecommuting and remote accessing protocols and procedures.
- Train employees on acceptable and unacceptable uses of the company computer system.
- Update security protocols to ensure that they are functioning properly.
- Restrict confidential company information to only those with a legitimate need to know.
- Consider written confidentiality and non-compete/non-solicit agreements for those employees who have access to confidential company information.
- Monitor employee use of the computer system, and discipline employees for violating computer usage policies.
- Include language rescinding any previous authorization for computer access on all termination notices and exit letters.
- Upon notice of an employee's resignation, immediately revoke all log-in and company email privileges.
- Upon termination or resignation, obtain all company issued computer equipment, including desktops, laptops, PDAs, Blackberry devices, etc., from the employee.
- Upon termination or resignation, preserve the employee's hard drive and check the hard drive for recent suspicious activity.

Baker Donelson stands ready to assist you with these and other employment-related challenges. For assistance, please contact your Baker Donelson attorney or any of our more than 90 attorneys practicing labor and employment law, 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.