CLIENT ALERT ARMSTRONG TEASDALE LLP

March 2010

Trade Secret Theft

You cannot afford to have your trade secrets and critical customer or technical information walk out the door. Armstrong Teasdale is partnering with companies to help them protect trade secrets, confidential information and customer relationships.

Would you benefit from a trade secret/non-compete audit?

A recent national survey reported that 59 percent of employees who quit or were laid off or terminated during the last 12 months *admitted to stealing company data*, and 67 percent *admitted to using their former employer's confidential data to find a new job*.

Unfortunately, breaches of non-compete agreements and agreements not to solicit a former employer's customers are becoming commonplace. Fortunately, there are many steps you can take to protect your trade secrets, confidential information and customer relationships. Audits of your current policies, practices, agreements, technology and patent procedures are critical for ensuring that the appropriate procedures are in place to protect your valuable information and relationships.

Shocking survey results

The survey, sponsored by Symantec (a global leader in providing data security, storage and systems management) included employees working in corporate information technology, financial and accounting, sales, marketing and communication and human resources and found that:

- 53 percent of departing employees stole data by downloading it to a CD or DVD
- 42 percent stole data by connecting a thumb drive to a computer
- 38 percent transferred data to a personal e-mail account
- 24 percent still had network access after they had left the company
- 82 percent of employers failed to audit or review what documents and data was taken
- The most commonly stolen items include e-mail lists, employee records, customer information and critical technical information

Employees who took confidential information offered various excuses including "everyone else does," "the information may be helpful in the future," and "the company can't trace the information back to me." This alarming increase in employee theft of confidential information is consistent with news reports, statements from the FBI and United States Department of Justice and our own experience.

What can I do about it?

Implementing a culture of protecting key business and technical information will enable the company to secure its future. For example, you should consider:

- Adopting a comprehensive policy to protect key business and technical information
- Marking confidential documents "Confidential"
- Making sure electronic data is appropriately protected with locks, passwords, or other appropriate restrictions on access, which limit access only to those employees with a need to access such information
- Adopting policies requiring return of all company documents and electronic data when requested and at termination
- Requiring employees and contractors to sign non-disclosure agreements. Such agreements may allow your company's attorneys to seek return of stolen data, a court injunction barring future disclosures, and recovery of your attorneys' fees
- Including provisions in employment agreements, separation agreements, consulting agreements and the like to maximize protection of key business and technical information
- Conducting periodic training to remind employees of their obligations
- Identifying and protecting key technical information with patents
- If you suspect an issue, immediately engaging the services of legal counsel to inspect records, laptops and computer systems so as to preserve the information and prevent your legal rights from being jeopardized

Properly conducted exit interviews can be critical

Conduct exit interviews of departing employees to verify that all company property, including computers, PDA's, documents and electronic data, has been returned. Consider obtaining written statements from departing employees certifying that they have returned all company documents, property and data and have deleted all e-mail and data files containing confidential company information located on any computers and PDA's owned by the employee.

During the exit interview, you should remind the employee of his/her obligations pursuant to any non-disclosure, non-solicit, and non-compete agreements and consider providing the employee with copies of all such agreements. Departing employees also can be reminded of federal and state computer tampering laws, including the federal Computer Fraud and Abuse Act, that impose civil and criminal penalties for exceeding authorized access to a computer and for obtaining or altering information in a computer that the employee is not entitled to obtain or alter. In addition, they can be advised that under the Uniform Trade Secrets Acts of Missouri and many other states, disclosing a company trade secret can result in the award of actual and punitive damages.

Absent a contrary business need, computer access should be terminated no later than the day and time the employee is terminated. In addition, every departing employee should be asked who he/she plans to work for after leaving your company. Any vague or suspicious answers should raise a red flag. It is rare for an employee to voluntarily resign unless he or she already has something else lined up.

Check with counsel to determine whether it is appropriate to notify the employee's new employer of the employee's non-disclosure and non-compete obligations.

Consider non-compete and non-solicit agreements

Consider non-solicit and non-compete agreements for employees who have an opportunity to develop close relationships with your customers and vendors, and for technical and other key employees who have access to your trade secrets. These agreements can often prevent, or at least deter, departing employees from soliciting your customers or unreasonably competing with you. If the employee is unable to work for a competitor, he/she may be less inclined to steal your confidential and technical information and customer data. Consider requiring employees to advise you of the name and address of all new employers during the post-employment period covered by the non-solicit and/or non-compete agreement. Also, consider prohibiting former employees from recruiting current employees or inducing them to resign from your company.

The employment laws of some states restrict the rights of an employer to mandate that an existing employee sign a non-compete or non-solicit agreement. Because courts can narrow or refuse to enforce overbroad or unreasonable agreements, consult with legal counsel to assess the best process to implement these agreements in the states where you have employees.

Trade secret/non-compete audits

Consider having one of our experienced attorneys conduct an audit of your policies, practices and agreements with employees. Because of our years of experience in litigating trade secret and non-compete cases in courts around the country and implementing procedures to protect and patent key technology, we believe that such an audit (which goes far beyond just reviewing your non-compete agreements) will likely reveal numerous additional steps that you can take to protect your company's most valuable assets — its trade secrets, technology and customer relationships. Our attorneys can help you institute the practices that are required in order for you to take advantage of the Uniform Trade Secrets Act, the Computer Fraud and Abuse Act, and various state computer tampering laws. Our attorneys can also help advise you on how to avoid being sued by another employer because you hired a worker who had signed a non-disclosure or non-compete agreement with a prior employer. Our attorneys can help you implement procedures to secure patent protection for key technical developments.

We urge you to contact your client manager or one of the attorneys listed below to discuss whether your company would benefit from a trade secret/non-compete audit. We have prepared a detailed checklist, which can serve as a good starting point to help us work with you to determine whether you have policies, practices or agreements that may need to be updated or improved. In these difficult economic times, when every company is fighting to maintain market share and customer relationships, you can ill afford to have your trade secrets and critical customer or technical information walk out the door. We believe that you will find the cost of such an audit very affordable and an excellent investment in your company's future.

Questions about this client alert can be directed to your usual Armstrong Teasdale contact attorney or any of the following attorneys:

Cary Levitt / 314-259-4748
clevitt@armstrongteasdale.com

Jeffrey Schultz / 314-259-4732
jschultz@armstrongteasdale.com

Michael Kass / 314-552-6673
mkass@armstrongteasdale.com

John Vering / 816-472-3114
jvering@armstrongteasdale.com

Larry Tucker / 816-462-3123
ltucker@armstrongteasdale.com

MISSOURI | KANSAS | ILLINOIS | NEVADA | SHANGHAI