Don’t Let Inattention Cripple Your Business: Simple Tips for Protecting Trade Secrets & Client Relationships

By John A. Vering & Brenda G. Hamilton **You are risking loss of valuable business information and customer relationships if your non-compete, non-solicitation and non-disclosure agreements are not effective and up-to-date with the law.** Few businesses can afford to have their trade secrets and critical customer or technical information walk out the door with an employee who plans to use that information to steal customers or otherwise compete against his or her former employer. When this happens, the results often can be devastating for the former employer. Can you afford to take this risk? If not, Seigfreid Bingham’s experienced employment attorneys are adept at helping companies prevent the theft of trade secrets, confidential information and customer relationships using various legal strategies. We advise clients to have legal counsel regularly conduct trade secret/non-compete audits, which is an effective strategy for reducing this type of risk at a relatively modest cost. Such an audit helps us identify and fix gaps and weaknesses in the scope and enforceability of companies’ existing non-competition, non-solicitation and non-disclosure agreements and related policies and procedures. And for companies who do not currently use such items, we assist them in evaluating whether to implement a non-disclosure, non-compete and/or non-solicitation program and draft the required agreements, policies and procedures.

Many companies would benefit from a trade secret/non-compete audit, given that the law in this area is constantly changing.

A recent national survey reported that 59 percent of employees whose employment terminated during the last 12 months admitted to stealing company data, and 67 percent admitted using their former employer’s confidential data to find a new job. Unfortunately, breaches of non-compete agreements, non-disclosure agreements and agreements not to solicit a former employer’s customers are becoming commonplace, and courts are unwilling to enforce such agreements if they do not comply with current legal requirements. Fortunately, there are many steps you can take to protect your trade secrets, confidential information and customer relationships and put yourself in the best position to convince a court to enforce these agreements when the need arises. Audits of your current policies, practices, agreements and technology procedures are critical for ensuring that the appropriate protections are in place to protect your valuable information and relationships.

Shocking survey results underscore the importance of making sure your agreements are effective and up-to-date with current law.

A recent survey of employees working in corporate information technology, financial and accounting, sales, marketing, communication and human resources fields that was conducted by The Ponemon Institute on behalf of Symantec (a global leader in providing data security, storage and systems management) found that:

- 62% of employees wrongly believe it is acceptable to transfer work documents to personal computers, tablets, smartphones or online file sharing applications. The majority never delete the data they’ve moved because they do not see any harm in keeping it.
- 56% of employees do not believe it is a crime to use a competitor’s trade secret information, although it often is; this mistaken belief puts their new employers at risk of being sued as unwitting

recipients of stolen IP.
- 44% of employees incorrectly believe a software developer who develops source code for a company has some ownership in his or her work and inventions, and 42% do not think it's a crime to reuse the source code, without permission, in projects for other companies.
- Only 38% of employees say their manager views data protection as a business priority, and 51% think it is acceptable to take corporate data because their company does not strictly enforce policies and agreements.
- The most commonly stolen items include e-mail lists, employee records, customer information and critical technical information.

Employees who had taken confidential information offered various excuses including "everyone else does it," "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 and customers is consistent with news reports and the experiences of our firm's intellectual property and employment attorneys.

What can I do about it?

When dealing with employee trade secret theft, an ounce of prevention is worth several pounds of cure. One of the most important things you can do to reduce your risk and secure your company's future is to implement a culture of consistently protecting the secrecy of your key business and technical information. For example, you should consider:

- Adopting and consistently enforcing a comprehensive policy to protect key business and technical information from disclosure
- Marking confidential documents "Confidential"
- Ensuring that electronic data and confidential documents are appropriately protected with passwords, locks or other appropriate restrictions on access, and allowing access only by those employees who need to use such information
- Adopting and consistently enforcing policies requiring the return of all company documents, electronic data, electronic devices and other company property when requested and at termination
- Requiring employees and contractors to sign appropriate non-disclosure agreements and then consistently enforcing the terms of such agreements. Such agreements may allow your company's attorneys to obtain the return of stolen data, a court order barring future disclosures, and even 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 by prohibiting employment with competitors and solicitation of customers, to the extent permitted by current law
- Conducting periodic training to remind employees of their non-disclosure, non-compete and non-solicitation obligations
- If you suspect an employee has stolen or is planning to steal your confidential business information or customers, immediately contact legal counsel to conduct an investigation that should include an inspection of relevant electronic communications, laptops and computer systems and mobile devices, among other things, so as to locate and preserve all evidence of the theft or planned theft. This will allow you and your attorneys to take effective, proactive steps to prevent or minimize the theft and its negative impact on your business, including potentially seeking a court order preventing such theft.

Properly conducted exit interviews are crucial.

Always conduct exit interviews of departing employees to verify that all company information and other property, including computers, electronic and mobile devices, documents, and electronic data have been returned. Consider obtaining written statements from departing employees certifying that they have returned all such information and property, and have deleted all e-mail and data files containing

confidential company information located on any computers and electronic and mobile devices personally owned by the employee. During the exit interview, you should remind the employee of his/her obligations pursuant to any non- disclosure, non-solicitation 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 Federal Defend Trade Secrets Act and the Uniform Trade Secrets Act 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 and email access should be terminated no later than the day and time the employee's employment ends. In addition, every departing employee should be asked to identify any new employer for whom he or she plans to work after leaving your company. Any vague or suspicious answers should raise a red flag and lead you to consult as soon as possible with legal counsel about how to proceed, as employees typically do not voluntarily resign unless they already have new employment lined up. It is important to act quickly if you believe a departing employee may be planning to work for a competitor, or may have stolen confidential information or solicited customers. This is because much of the damage to your business that can result from such activities typically occurs in the first few days and weeks following the employee's departure, with customer solicitation often beginning immediately upon, or even before, the departure. *Check with legal counsel to determine whether it is appropriate to notify the employee's new employer of the employee's non-disclosure, non-compete and non-solicitation obligations, as taking this step is often an effective way of preventing or limiting the damage from a departing employee's theft of your confidential information and improper solicitation of your customers*. Consider including in your employment, severance, contractor agreements and other similar agreements a provision giving you the right to notify the employee's new employer of these obligations.

Require key employees to enter into non-compete and customer non-solicitation agreements.

Employees who have had an opportunity to develop close relationships with your customers and vendors or who have access to your trade secrets and other confidential information should be asked to sign non-compete and/or customer non-solicitation agreements. These agreements can often prevent, or at least deter, departing employees from soliciting your customers or wrongfully competing with you by using your confidential information. If the employee is contractually barred from working for a competitor, he or she may be less inclined to steal your trade secrets and other confidential information and may lack incentive to steal your customers. Consider requiring employees to advise you of the name and address of all new employers during the post-employment period covered by the non-solicitation and/or non-compete agreement. Also, consider prohibiting former employees from recruiting current employees or inducing them to resign from your company by including a provision to that effect in the non-compete and/or non-solicitation agreement. The laws of most states allow an employer to require new or existing employees to sign a non-compete or non-solicitation agreement as a condition of employment and provide that such agreements are enforceable against the employee so long as they are properly drafted in compliance with the current law. Because courts may narrow or refuse to enforce such agreements when they don't comply with applicable law, you should consult with legal counsel to ensure your agreements comply with current law.

Schedule a trade secret/non-compete audit.

Consider having one of our experienced employment attorneys conduct an audit of your policies, practices and agreements with employees, contractors and vendors. Due to our employment attorneys' many years of experience in drafting policies and agreements designed to protect businesses' confidential information and customers from theft and litigating trade secret and non-compete cases in courts around the country, we believe that such an audit will likely reveal additional steps you can take to

increase the protection of your company's most valuable assets – its trade secrets, technology and customer relationships. Our attorneys also can help you institute practices that are required to take advantage of protections offered by the Uniform Trade Secrets Act, the Computer Fraud and Abuse Act, the Defend Trade Secrets 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 have hired or are considering hiring a worker who signed a non-disclosure, non-solicitation or non-compete agreement with his or her prior employer. We urge you to contact your existing attorney or one of the experienced employment 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 efficiently to determine whether you have policies, practices or agreements that may need to be updated or improved. In these economic times when every company is fighting to maintain market share and customer relationships, you cannot afford to have your trade secrets and customers leave with an employee who plans to compete against you. 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 Seigfreid Bingham contact attorney, or any of the following Seigfreid Bingham employment attorneys:

John Vering / 816.421.4460 jvering@sb-kc.com Brenda Hamilton / 816.421.4460 bhamilton@sb-kc.com Rachel Baker / 816.421.4460 rbaker@sb-kc.com John Neyens / 816.421.4460 jneyens@sb-kc.com