FINANCIER WORLDWIDE corporatefinanceintelligence

HUNTON& WILLIAMS

WORLDWATCH

US LABOUR & EMPLOYMENT LAW

Keeping the cat in the bag: protecting company trade secrets and confidential information in an age of increased employee mobility

www.financierworldwide.com

FW MAGAZINE

REPRINTED FROM

September 2009 Issue

TEXAS

Keeping the cat in the bag: protecting company trade secrets and confidential information in an age of increased employee mobility

BY LAURA M. FRANZE, DAVID C. LONERGAN, AND ALAN J. MARCUIS

When your employees walk out the door for the last time, they may be taking more than their personal belongings. Increased employee mobility, whether occasioned by corporate raiding or an economy-driven reduction in force, puts your top talent, customer relationships and trade secrets at risk. Unscrupulous workers, especially when equipped with remote computer access or tiny electronic storage devices, make it increasingly difficult for businesses to safeguard corporate assets. Theft and misappropriation of trade secrets, customer lists, and other intellectual assets is estimated to cost US businesses $250bn a year, with employees, especially those about to jump ship, accounting for much of this loss. Theft included in this figure might take the form of an employee who emails himself confidential pricing information just before announcing his resignation, or the employee who surreptitiously downloads information about breakthrough technology in development. It does not include, however, the almost incalculable relationship and training-investment losses that occur when key employees are poached specifically for the institutional information and/or customer relationships they developed on their former employer's payroll.

Given the money involved, it is no surprise that lawsuits abound on both sides of the equation. Employers may be forced to file suit to protect themselves from departing employees and data leaks. They must also take care when hiring a competitor's employees that they do not end up defending a similar lawsuit. Proactive formulation of internal controls, policies, contracts with key employees, and an active enforcement plan, however, can enhance protection for a company's informational assets and greatly reduce the need for litigation.

Consider the following examples. Before resigning, a key sales employee downloads your customer and pricing lists – can you stop use of this data? Another departing employee sends an email to a personal email address containing important research and a timetable for planned product upgrades. Unbeknownst to you, a third employee is using company resources to develop technology that would be useful to your company, and takes it with her at departure – who owns it? A competitor specifically targets your top employees in an attempt to cripple or slow your growth, and uses sources inside your company to recruit – what are your rights? You discover anonymous blogging or social networking posts revealing sensitive company information accessible only to employees – what are your options?

Answers to these questions depend on a complex web of employment, privacy, corporate, criminal, and business tort law – both statutory and case based – that varies from state to state. For each situation, the outcome may differ depending on the jurisdiction and, more importantly, on what proactive steps an employer has taken to protect its confidential information and keep the proverbial cat in the bag.

Tying up the bag: enhancing employer interests through policies, contract provisions, and security measures

Employers may enhance or clarify rights and expectations by policy or contract. Published employment policies, orientation guides, and handbooks, for example, can be used to define duty-of-loyalty restrictions on use or dissemination of a company's confidential information, and these restrictions can be reiterated and transformed into specifically enforceable rights in individual employee contracts. In our hypothetical, the departing employees' contracts should include post-employment non-disclosure covenants concerning trade secrets and confidential information and non-solicitation and non-competition covenants to prevent the employees from soliciting the company's employees and customers for specified periods. The covenants should define the company's protectable trade secret and confidential information interests broadly; have the employee acknowledge the company's investment in and steps taken to protect the information and agree that the protected information gives the employer a competitive advantage; have the employee acknowledge that he or she is not violating any restrictions from prior employers or improperly using their confidential information; obligate the employee post-termination to inform the company when he or she goes to work for a competitor; and require the employee to inform future employers of his continuing obligations to the company.

Policies or contract language protecting an employer's proprietary information should be backed up by company security procedures, including IT protocols. Depending on the nature of the information to be protected, companies may consider implementing a combination of measures, for example, locking offices, file cabinets, storage and computer rooms in which confidential information is located and limiting access to these areas to employees with a legitimate need to know; using biometric, retinal, or other employee-specific access devices that can monitor and track who accesses the company's confidential information, when, and where; appropriately labelling all confidential information and, for electronically-stored information, using 'pop-up' acknowledgements that appear each time such information is accessed reiterating the confidentiality of the information and reminding the employee of his or her non-disclosure obligations; and encrypting all computer hard drives, data storage devices, and electronic communications that contain confidential information.

Security procedures serve a dual purpose. Under most states' laws, an employer must take reasonable security measures to protect the confidentiality of its confidential information so that it continues to confer a competitive advantage on the employer or risk losing the information's protected status. Thus, not only are security procedures a direct line of defence against theft of information, but the existence of such protocols is a required element of an employer's claim that the protected information constitutes a legitimate, protectable trade secret and was intended to be proprietary. Effective enforcement protocols also must be informed by forensic considerations appropriate ▸▸

to your business.

Employer and employee obligations discussed thus far vary in detail only minimally from state to state. Interstate differences are more dramatic, however, in the case of post-employment covenants not to compete. Such covenants are popular with employers because they often provide the surest form of protection from poaching of key employees and the intentional or inadvertent leak of proprietary information by flatly prohibiting an employee from taking employment with competitors for a specified period of time. Non-competition covenants are most often used in employment contracts for key high-level or strategic positions and to prevent poaching of employees in whom the company has made particular investments (for example the key sales employee described in our hypothetical).

While covenants not to compete are often the most effective protection of corporate investment in human capital, such covenants are also fraught with litigation potential and uncertainty. Employers asserting non-competition covenants generally must demonstrate that they protect legitimate business interests and are reasonable as to time, geography and scope of activity restricted. What is 'reasonable' is not only a fact-based inquiry, but can also vary based on individual state rules or custom. While most states, including Texas, will enforce properly and narrowly drawn covenants designed to protect legitimate business interests, other states, including most notably, California, will reject almost any contractual restriction on future employment as void. In Texas and several other jurisdictions, detailed technical requirements for enforceable non-competition agreements in employment contracts are set forth by state statute.

Multi-state employers and companies with employees who work across state lines also confront 'choice of law' problems that require them to determine which state's laws they legitimately can and should designate as controlling the interpretation and enforcement of restrictive agreements. A company must first identify those states with a sufficient connection to the employment relationship to apply their law to disputes involving the employee's contractual obligations, and then assess from those options which state's laws are most favourable to them. Because employment rights are considered a matter of public policy, states generally favour applying their own laws in this area. However, courts also look to other factors including the situs of employment (former and prospective), location of the employer, the location where the contract was executed, contract language, and other factors. As a practical matter, resolution of choice of law issues may also depend on who gets to which courthouse first. In some cases, data breach or breach of covenants can also involve cross-border issues.

What to do if the bag leaves the building: enforcing rights

Even the most refined contract terms and internal policies will mean little if an employer is not diligent about enforcing its rights. And what happens in the early days of a breach can make a big difference. Whether the issue is an illegal download of confidential information or breach of a post-employment covenant, quick action is essential to minimise damage. In some cases, restraining orders can and should be obtained on an emergency basis. Where theft or criminal privacy interests are implicated, law enforcement authorities should be consulted. Third parties should be put on notice of company interests and claims and, if appropriate, cease and desist letters deployed. Companies can also take practical steps upon learning that employees are leaving, such as monitoring their computer activities, limiting their access to confidential information, and conducting exit interviews during which departing employees are reminded of their non-compete, non-solicitation, and non-disclosure obligations.

The above measures are not 'magic bullets' that will ensure the safety of a company's protected information. In combination, however, they will increase the likelihood that a company's information will remain protected and better position the company to respond should it discover that a former employee is planning to 'let the cat out of the bag.' ■

This article first appeared on www.financierworldwide.com in *September 2009*.

Laura M. Franze
Co-National Section Head, Labour and Employment
Dallas, Texas
T: +1 (214) 468 3516
E: lfranze@hunton.com

Laura M. Franze (Dallas and Los Angeles), co-Chair of the Labour and Employment group, maintains a national complex employment practice focusing on class, collective, and mass action litigation across the country, particularly in Texas and California. She is the author and Editor in Chief of Texas Employment Law (James Publishing).

David C. Lonergan
Partner
Dallas, Texas
T: +1 (214) 979 3061
E: dlonergan@hunton.com

David C. Lonergan (Dallas) focuses on representing employers in federal and state court proceedings, counselling clients on day-to-day labour and employment matters, structuring corporate reorganisations to avoid employment law pitfalls, including developing objective selection criteria, exit incentives, preparing retention and employment contracts, and designing executive compensation.

Alan J. Marcuis
Partner
Dallas, Texas
T: +1 (214) 979 3060
E: amarcuis@hunton.com

Alan J. Marcuis (Dallas) advises management on labour and employment law matters, including trade secret and non-compete litigation, EEO litigation, collective bargaining, union avoidance, and preventive employee and labour relations consulting. He has twice been named a Texas Rising Star.

Hunton & Williams LLP is a US based law firm with 19 offices across the globe. Since our establishment more than a century ago, Hunton & Williams has grown to more than 1000 lawyers in the United States, Europe and Asia, with extensive experience in Africa and South America. We provide our clients with experience, advice, and a diverse array of legal services in virtually every discipline of the law. We can respond knowledgeably, effectively, and quickly, whether the issue is local, regional, national, or international. While our practice has a strong industry focus on energy, financial services, and life sciences, our experience extends to more than 100 separate practice areas, including bankruptcy and creditors rights, commercial litigation, corporate transactions and securities law, intellectual property, international and government relations, regulatory law, labour and employment products liability, and privacy and information management. Our client base ranges from entrepreneurs to Fortune 10 corporations to global biotech innovators. Consistent with a firm that claims a former US Supreme Court Justice as an alumnus, Hunton & Williams is consistently listed among the most highly ranked law firms by The National Law Journal, Thomson Financial, Chambers, BTI Consulting, and others; and has achieved a national reputation as a pro bono leader among large law firms. For additional information, visit www.hunton.com.