

SMART BUSINESS[®]

INSIGHT. ADVICE. STRATEGY.™

DALLAS

SMART LEADERS

Entrust's Bill Conner on why sometimes you have to sacrifice a limb to save the body

FAST LANE

How Carol Roehrig stays close to the customer at BKM Total Office of Texas

Rules of engagement

MIKE KEEBAUGH CHALLENGED RAYTHEON INTELLIGENCE AND INFORMATION SYSTEMS' 9,000 EMPLOYEES TO ACHIEVE EXPLOSIVE GROWTH

Make sure you're protected

Protecting intellectual property from employees **Interviewed by Curt Harler**

Commercial entities such as banks, retailers and airlines know that some of their own employees are far more likely to steal from them than is a thief from outside of the organization breaking into their facilities. This "likelihood" also ports to companies that own or manage intangible assets — ideas, know-how, confidential information, inventions (patented or not), works of authorship protectable by copyright, trade secrets, trademarks, trade dress, business methods and patents.

"Employees can do serious damage to a company's future if they walk off with their employer's intellectual property, particularly its confidential information, including trade secrets," says William Munck, chairman of the Dallas-based law firm of Munck Carter, P.C.

Smart Business talked to Munck to find out how a company can better protect its trade secrets and other intangible assets.

What is a 'trade secret'?

Trade secrets may be thought of as any information having independent economic value that is not generally known or otherwise readily ascertainable. Examples of trade secrets may be ideas, patterns, compilations, programs, formulas, methods, techniques, processes and secret devices. The courts also have found such things as machining processes, blueprints, computerized stock trading systems, customer lists, pricing information, unpublished inventions and nonpublic financial data — overhead rates and profit margins — that help companies price their goods and services to be trade secrets.

Can companies prevent exiting employees or contractors from stealing trade secrets and other IP when they leave the company?

It is impossible to prevent all trade secret theft by exiting employees or contractors. The situation is unfortunately exacerbated when a company fails to take appropriate precautions. Some tools at the company's disposal include requiring employees and contractors, when they are engaged by the company, to sign engagement agreements, including (i) broad nondisclosure provi-



William A. Munck
Chairman
Munck Carter, P.C.

sions and (ii) narrow noncompetition provisions that cooperate to prohibiting the employee or contractor from using company confidential information to compete with the company; educating employees and contractors about trade secrets and other IP and the importance of keeping confidential information, such as trade secrets, confidential; conducting exit interviews with departing employees and contractors to remind them of their duty to keep confidential information secret; limiting access to confidential information to those who need to know; and employing electronic surveillance equipment and software to limit and monitor access to confidential information.

Are noncompete agreements enforceable?

Frankly, they must be appropriately narrow in scope to be enforceable. This means that provisions must be limited, such as to geographic areas, scope of employment and duration in time. It is always recommended that such terms be included in an initial engagement/employment agreement that is

WILLIAM A. MUNCK is chairman of the Intellectual Property section at Munck Carter, P.C. He concentrates his practice on domestic and foreign IP procurement, exploitation, enforcement and counseling. Dedicated to counseling clients concerning their development of offensive and defensive IP portfolios, Munck emphasizes market-focused long-range corporate strategies for private financing, public offerings, mergers, acquisitions and establishing market leadership. Reach him at wmunck@munckcarter.com.

executed by the employee/contractor and the company at the start of the relationship.

In the event that such language is not initially included, and the company decides that it is desirable later on to include such terms, the situation is more complicated. To add not-to-compete covenants into existing agreements, there must be additional and adequate consideration exchanged between the employee and the company for post-employment obligations.

With little USB drives, is it easy for current employees to walk off with files?

While USBs are a new tool for stealing confidential information, they are only slightly different than e-mail or other tangible mediums for copying the same. The real question is, "What can a company do about an attempted or actual misappropriation of confidential information or other IP?"

The company must immediately pursue injunctive relief to prevent an attempt to misappropriate confidential information from becoming an actual disclosure of the same. While such action involves retaining an attorney and filing a lawsuit, it is often necessary because once the confidential information, particularly the trade secret information, is made public, it is much more difficult, if not impossible, to restore the information to trade secret status.

It is important to note that pursuing monetary relief due to corporate misappropriation of confidential information may be more practicable. Most jurisdictions actually permit recovery of both the actual loss caused by the misappropriation as well as any unjust enrichment gained by the wrongdoer as long as the 'enrichment' is not included within the 'actual loss' portion of the analysis. If such damages are not easily proved, the company may seek to impose a 'reasonable royalty' damage model. If the conduct leading to the misappropriation was willful, most jurisdictions permit the awarding of punitive damages and the award of attorney's fees. <<

Insights Legal Affairs is brought to you by Munck Carter, P.C.