



## Protecting Your Intellectual Property Before a Key Employee Leaves

BY DAVID CHRISTOPHER BAKER, Esq.

The departure of a key employee, whether on good terms or bad, can be a stressful time for any management company. There are a myriad of issues to address including such things as severance packages, COBRA benefits and the transition of open matters to continuing employees. But, one of the most difficult aspects of an employee separation is the proper handling of Intellectual Property (IP). Key employees/principals, by the very nature of their importance to the management company invariably have access, often times, unlimited access, to key company information and data. This information or IP usually takes the form of trade secrets and can consist of client and contact information, prospects lists, goods and services parts and pricing lists, business protocols and procedures and a virtually unlimited number of other proprietary information. Other forms of IP, such as copyrights, trademarks and patents, are usually not an issue in an employee separation because their ownership and registration have been well-documented and clearly remain the property of the business during and following a key employee departure. However, it is critically important to a management company to prepare for the departure of even its most important employees.

In order to function the management com-

pany must allow key employees access to IP. This doesn't mean that access should be unfettered or unmonitored, and it certainly does not mean that employees should be allowed the opportunity to copy, alter or even delete such information with impunity. You must institute and regularly enforce your IP protection protocols so when a departure occurs, whether it is voluntary or involuntary, the management company is prepared to handle the departure with a minimum of interruption of your daily business.

Virtually every business is subject to attack from within, and after a key employee departure, there is often a dispute over ownership and control of key contacts and client files. A couple of common sense steps YOU can take to avoid this happening to you and your business are:

1. When a key employee talks about their departure from prior employment, listen and learn from their comments.

2. When an employee expresses dissatisfaction with their job, listen carefully. Employees who are unhappy at work often will talk to co-workers and sometimes even upper management about their plans for the future. While these comments often appear to be simple gripes, there are nuggets of truth which can reveal actual plans. Look for these subtle clues and use them to lock down that employee's access to your IP and limit any po-

tential damage.

**Know Your IP!** Any business or management company that does not know what information is most important to their business cannot protect it. If files are open to every employee in the organization, it is virtually impossible to maintain their integrity in the event of a key employee departure. If there is no monitoring system for access to that information or to routinely verify its very existence, the same holds true. The information is vulnerable to attack.

**Implement Reasonable Security Measures!** While this is obvious, such things as locks on doors and encrypted passwords on computers and limited handling of confidential hard copies can be easy, cost-effective ways to protect the integrity of your IP. A good IT professional can assist you in establishing protocols that will monitor the use of information, back it up and limit any destructive intent by a departing employee.

**Know Your Ethical Obligations!** Most businesses have mandated ethical standards they must maintain to protect their information, such as sensitive client information, credit and credit card data, the identity of minors, etc. Don't be fooled into thinking that a key employee by virtue of their title will respect the integrity of such information merely because of the requirement that he or she adhered to a code of ethics or conduct.

**Document-Document-Document!** Often when a disgruntled employee is planning to leave, they will start plotting their strategy—copying documents, downloading files, etc. There are always signs that an employee is get-

**The departure of a key employee, whether on good terms or bad, can be a stressful time for any management company.**

ting ready to leave, and you will know what they are for your business. Watch for those signs, take note and report immediately up to the chain of command, and most importantly—take action. After meetings are conducted, draft a confirming document for management personnel to review. Management should be informed of any decisions by the higher chain of command that affects both the employee's continued employment and his or her access to the management company's IP.

**Lock Down All Access at Termination.** Although this is fairly obvious, this is a very important final step in securing your IP. You need to change passwords, collect keys and retrieve pass cards or any other forms of data access. Exiting employees should not be allowed access to company property, in particular computers, file management systems and hard copies, once management is aware of their impending departure. This is critical to the integrity of your management company's IP. If after the termination of the employment relationship, there is a breach, it will most likely be considered a crime and the property authorities can be notified.

**Damage Control.** This includes informing clients about the transition, providing press releases to local and industry publications—if applicable, and posting to our management company's website. After a departure, a management company should be sensitive to signs that data has been lost or compromised—such as sudden client departures, unsolicited phone calls, unexpected complaints about issues of which you were unaware.

\* \* \*

There is no "magic bullet" to prevent a key employee from abusing their access to sensitive corporate or business IP. The nature of this relationship makes it impossible. But—a business or management company that is sensitive to its obligations and has the proper internal controls in place, will be able to minimize any detrimental effect resulting from a key employee's depart-

ture. The end of an employment relationship with a key employee does not have to be the end of time for a business.

*Dave Baker is partner with the California law firm of Hart, King & Coldren. He has over 25 years of wide ranging Intellectual Property protection and enhancement, commercial transactions and litigation and real property litigation. Dave can be reached at (714) 432-8700 or at dbaker@hkclaw.com. Dave hosts a series of monthly IP Webinars, the next of which is scheduled for Wednesday, December 11, 2013 at 10 am PST) – Trade Secrets & Non-Disclosure Agreements. If you are interested in registering for this webinar or the 2014 IP webinar series, please email Barbara Ericson at (714) 432-8700 or at bericson@hkclaw.com.*

*visit our website at:*  
[www.journalmfdhousing.com](http://www.journalmfdhousing.com)

# Reil Rock

*Seamless Rock Skirting System*

Now available in

- Brown & Gray
- 32", 36", 48" heights
- easy installation

Accessories include:

Vent Inserts...  
that open & close

Access Doors...  
adjustable heights

Reil Rock ... "The Reil Thing"

REIL ROCK PRODUCTS, INC.

11 Reil Rock Industrial Blvd. Eufaula, OK 74432

800-242-3005

Pat. No. 4,944,124 Pat. No. 4,656,722

MPX

MERCHANT PRO EXPRESS

Lower Your Monthly Credit Card Processing Fees

We have the lowest rates in the industry and 24-hour service

Start Collecting Rent with Credit Cards

- Free Setup
- Decrease Tenant Late Payments
- Simplify the Rent Collection Process

Call Today!

Emily Kozitsky  
(585) 423-0256  
ekozitsky@mproexp.com