CORPORATE IDENTITY THEFT: A TRUE CRIME STORY

July 13, 2015 | Alert

For this discussion, let's assume that your business operates nationwide with offices in several states. Assume further that servicing your customers is heavily dependent on key employees serving a region from your local branch. And finally, assume that you have invested millions of dollars and years of your life building not only your nationwide brand, but the regional business serviced by this critical local branch.

One day, you discover that key employees from one regional office have formed a company with a name deceptively similar to your trade or business name (even though it's subject to state or federal trademark protection), and have begun actively diverting your company's business to their new company. Adding insult to injury, while still on your payroll, they download your key customer files and other proprietary data, though they do attempt to cover their electronic tracks.

Finally, they distribute letters to key customers on their attorney's letterhead, declaring that your company is not authorized to do business in the state where their business is located.

When your "foreign registration" with one secretary of state's office expired due to the tardy filing of a $30 renewal form, these employees create a new entity in that state using your company name, effectively blocking your reinstatement there.

This is not fiction, but fact! The foregoing plot comes directly from allegations in a case just initiated by this author to halt the deliberate, premeditated theft of one company's key branch.

No business owner or investor can sit idly by as their own employees pull the very rug out from under them — and attempt to sell it to his own customers! The business must recover the loss of its property, customers, and the corresponding revenue.

RELATED PROFESSIONALS

Frederic A. Mendelsohn

RELATED PRACTICE & INDUSTRIES

Corporate

Litigation

From a business and legal viewpoint, the company must also ensure that the word within the organization is that the owners will not tolerate such misconduct — lest other employees in different locations get similar ideas. As such, suit must be filed and aggressive litigation action taken.

Legal maneuvers have included temporary restraining orders and preliminary injunctions based on violations of the Unfair Competition Rules existing under the federal Lanham Act, the federal Computer Fraud and Abuse Act, and state laws prohibiting deceptive trade practices, trade secret misappropriation, interference with established business relationships, fiduciary duty violations, and conspiracy.

From a legal standpoint, it is worth noting that, in the case described here, none of the key malefactors had signed a covenant not to compete or any other post-employment restrictive covenant limiting post-employment solicitation and/or interference with business relationships (customer, vendor, employee).

How do such crimes happen? And, what can be done to prevent them?

In our experience, even with post-employment restrictive covenant agreements in place, many employees in such cases convince themselves that their agreements can simply be ignored or are not enforceable. These conclusions are often aided by attorneys advising that the non-compete agreement is illegal or can be defeated in court.

Nevertheless, post-employment restrictive covenants are valuable tools for preventing this kind of misconduct, and employment files should be regularly reviewed by your counsel to ensure that proper agreements are in place — to protect legitimate interests of customers, vendors and employees, as well as proprietary information, whether stored electronically or in paper files.

In light of the ever shifting landscape of the law on post-employment restrictive covenants (currently leaning toward limiting employers' power to protect their businesses), employee agreement audits should be undertaken on a regular schedule, and upgrades made as necessary to protect legitimate business interests to the ultimate extent of the law. A state-by-state analysis can prove critical.

Similarly, a detailed calendar must include dates concerning regulatory requirements — early warnings of foreign entity registration and business license renewal deadlines should be on the company calendar, along with tax filings and insurance payments.

The same holds true for state and federal trademark registrations. Maintaining federal trademarks can involve the timely filing of Affidavits of Continued Use (a sworn statement filed by the owner of a registration that the mark is in use in commerce) and payment of fees; state level requirements vary. Assumed business names and similar filings must also be regularly audited for continued compliance with state requirements and fee payments.

And last but not least: ALL businesses have proprietary information, some of which may qualify as protectable trade secrets. An annual check-up on the nature and secure storage of such information, policies and agreements related to the use, access and maintenance of these assets, is likewise critical to the ongoing security of any business.

Fred Mendelsohn would be happy to answer any questions regarding this subject matter. He can be reached at fmendelsohn@burkelaw.com or 312/840-7004.