The Confidentiality of Commercially Valuable Information

Peter Bowal and Leo Dragos

Introduction: the Cymbal Business

In an age when multi-billion dollar companies struggle to survive, a small family-owned company called Zidjian continues to manufacture cymbals as it has for almost four hundred years. It controls almost 65% of the world's cymbal market, with annual revenues close to $50 million. The formula of the special alloy used to manufacture these cymbals is even kept from family members until their trust is earned.[1] If the Zidjians had protection for the alloy formula through a patent, that protection would have expired and their business viability would have been lost long ago.

The protection the Canadian legal system can offer through intellectual property (copyright, patent, trademark and industrial design law) is limited in scope and time. Businesses mightily relying on valuable information may be better off doing what the Zidjians did: protect that information from disclosure through their own efforts.

Risk of Unauthorized Employee Disclosure and Mis-Use

Commercially valuable information must be carefully protected today. Employees collectively represent one of the greatest risks to unauthorized disclosure of valuable information. Inadvertent disclosure, such as accidentally leaving a memory stick at an off-site meeting, can be planned for and mitigated to some extent by appropriate training and embedded locks. Deliberate disclosure is best prevented by meticulously selecting and monitoring employees and limiting their access to sensitive

information. The main protective legal instrument is the employer – employee confidentiality agreement. Ultimately, however, once valuable information has been improperly disclosed, it is impossible to get it back. It is very difficult practically to limit its further dissemination, even with an injunction, or to receive adequate compensation for the disclosure. The best approach is prevention.

Commercially valuable information must be carefully protected today. Employees collectively represent one of the greatest risks to unauthorized disclosure of valuable information.

Today's highly competitive business environment encourages employees to continuously seek better rewards for their skills by moving between jobs and companies, often in the same industry and geographical area. This adds to the challenge of protecting confidential information because employees are often hired for what they know. Organizations bleed information with each employee who resigns to take a job with a competitor.

As with the breach of contracts in general, the remedies sought for breach of confidentiality may be an injunction to stop further exploitation of the confidential information, but more often, monetary damages for lost revenues.

The Nunes Case

John Nunes was the manager and long-serving employee of Graham Funeral Homes (Graham), the only funeral home for the 10,000 people living in Oliver and nearby Osoyoos, British Columbia. In 2008, after he had made several unanswered offers to buy the business from the owner, Service Corporation International Canada Ltd. (SCIC), Nunes resigned. Together with Pottinger, the only other full-time employee at Graham, Nunes opened a competing business, Nunes-Pottinger Funeral Service & Crematorium Ltd. (NP). SCIC alleged Nunes and Pottinger, before their resignations from Graham, made copies of the existing pre-need client files and used that information for unfair competition, soliciting Graham customers who transferred 208 pre-need contracts to the upstart NP. SCIC sued for breach of contractual and fiduciary duties and claimed $551,000 in damages for lost profits and more for punitive damages (*Service Corporation International (Canada) Ltd. (Graham Funeral Home Ltd.) v. Nunes-Pottinger Funeral Services & Crematorium Ltd.* , 2012 BCSC 586).

Nunes pointed to his reputation in the small communities he served for more than 20 years. He said the Graham client contact information was immaterial to NP's success in attracting these former Graham clients. The defendants admitted to copying SCIC files but said those clients would have followed them to their new business in any case.

In April 2012, the Supreme Court of British Columbia found the defendants NP, Nunes and Pottinger jointly and severally liable to SCIC in amount of $280,285 as compensatory damages and punitive damages of $10,000 against Mr. Nunes. It was not the mere possession of SCIC's confidential information that mattered, but how the defendants used that information to deprive the rightful owner of it and, in the process, obtain undeserved benefits. Even where

Organizations bleed information with each employee who resigns to take a job with a competitor.

NP only used the names and the insurance policy numbers to eventually transfer these clients to their new business, this use of the former employer's information was illegal. Mis-use of proprietary confidential information opens the door to punitive damages "if, but only if, compensatory damages do not adequately achieve the objectives of retribution, deterrence and denunciation." (Performance Industries Ltd. v. Sylvan Lake Golf & Tennis Club Ltd.).

The best an employer can do is to have an enforceable confidentiality agreement entered into at the time of hiring.

Conclusion

Throughout history, being possessed of knowledge and information superior to that of one's competitors has been critical to military, political or business success. Employers enjoy a competitive advantage when they own technologies and processes that their competitors cannot easily replicate. Computers and photocopiers can collect, sort and store tremendous amounts of data that can be readily transferred into unauthorized hands. Employers have a *property* interest in this information which they have generated. Commercially valuable information is a valuable corporate asset, just like a unique high-demand product or service, a dedicated and skilled set of employees or well-located real estate.

The best an employer can do is to have an enforceable confidentiality agreement entered into at the time of hiring. This will discourage departing employees from taking valuable information with them when they resign their employment. An employee should depart a job with nothing more than what may be stored in his or her head.

As the recent *Nunes-Pottinger* case shows, an employer may be able to recover damages for the breach of implied duty of confidentiality, especially where the departing employees were originally entrusted with the valuable information and themselves personally gained from its misappropriation.

Employers and employees alike should be reminded of how the cymbal business continues to both make lovely music and remain resolutely quiet at the same time.

Notes

1 http://www.bbc.co.uk/news/business-18261045

Peter Bowal is a Professor of Law and Leo Dragos is an MBA student at the Haskayne School of Business, University of Calgary in Calgary, Alberta.