You Can't Take It With You? Ontario Court Clarifies Post-Employment Liabilities And Obligations For Employers And Employees

One of the most time consuming and costly areas of employment law concerns the obligations departing employees owe their employers, and how employers can protect themselves from a departing employee's breach. In *Titus v Hack*, the Ontario Superior Court clarified the various duties employees owe their former employers, and the consequences for breaching them. The case also warns employers it is not enough to prove a breach occurred; employers must also prove the damages they suffered because of the departing employee's breach.

In 2016, after approximately 15 years of service, Wayne Hack ("Hack"), a Vice President with Titus Steel Company Limited ("Titus"), resigned and started working for a competing business. Prior to his resignation, Hack downloaded Titus' business records, provided them to the competitor, and deleted Titus' records from its computer systems. After learning of Hack's activities, Titus commenced litigation claiming (among other things) that Hack breached the various fiduciary obligations he owed, improperly solicited Titus' customers, and that it was owed significant damages stemming from Hack's breaches.

Prior to determining whether Hack breached his post-employment obligations, the Court first considered whether Hack owed Titus any "fiduciary" obligations, given his senior title. To do so, the Court applied the "key employee" test and examined whether Hack: (i) was an integral and indispensable part of Titus' management team; (ii) was involved in Titus' decision-making processes; and (iii) could impair Titus' competitive advantage by his access to and disclosure of Titus' confidential information. The Court concluded that despite Hack's senior title, he did not owe Titus any fiduciary obligations because his job duties were more akin to a salesperson (a position which is not typically viewed by Courts as having fiduciary responsibilities). In particular, the Court found that Hack operated under the close supervision, and direction of Titus' owner and exercised little discretion in his day-to-day activities.

Nevertheless, and even though the Court found Hack did not owe Titus any fiduciary obligations, it recognized that as a former employee of Titus, Hack still owed duties of good faith, loyalty, and fidelity (duties all employees owe to their employers, regardless of their seniority, status, or title). As such, the Court found that Hack breached his ongoing obligations when he gave Titus' business records to a competing

business. However, of the 1000 documents Hack used to benefit his new venture, the Court determined only 2 documents contained Titus' confidential and proprietary information. In addition, Titus failed to prove that Hack's breaches resulted in lost customers or revenues, or that Hack's new business profited from his access to Titus' confidential information. The Court commented: "*There was no evidence that [Titus] began losing money, lost revenue or lost any customers. One would expect that the loss of an employee that was so key that he would be considered a fiduciary, would have such impacts, at least in the short run*". For all of these reasons, the Court awarded Titus no damages stemming from Hack's breaches.

While the Court's costs decision has not yet been released, *Titus v Hack* is a reminder that succeeding in "post-employment breach" litigation requires employers to prove: (i) that a breach occurred; and (ii) that it suffered financial or reputational damage because of the departing employee's breach. This case also warns departing employees that while Courts might not find them liable for post-employment breaches (absent evidence of damages suffered), they could be required to expend substantial time and resources defending themselves in costly and protracted litigation (in this case, judgment occurred 8 years after Hack's alleged breach).

Departing employees should therefore exercise caution when exiting an employer and avoid the following activities: (i) taking information or documents containing information their former employer might view as confidential or proprietary (including, but not limited to, customer lists, marketing plans, or pricing strategies); and (ii) contacting former clients or employees to advise of their new venture. Employers can protect themselves by reminding departing employees of their post-employment obligations and requiring departing employees to return all property and records (including electronic records). In the event of an anticipated or suspected breach, employers should also advise their former employee to cease and desist any improper activities, warn that they reserve the right to seek all available legal remedies, and closely monitor any business losses resulting from the departing employee's actions.

Author: Jeff Rochwerg

Turnpenney Milne LLP