Reaching Out

Reaching Out – Third Edition

Date: May 21, 2013

Dear Friends,

As we welcome back Spring, which finally seems to be taking hold, it presents an opportunity to do some spring cleaning and dust off common HR issues that bear review before we get too far into 2013.

In the Spring edition of *Reaching Out*, Carolyn Cornford Greaves, an associate in our Toronto office and member of Hicks Morley's Pay Equity group, discusses the implications of pay equity on collective bargaining. All too often, in an effort to "get the deal done" issues of pay equity are overlooked. Pay equity, however, can have significant financial implications for an organization, particularly where the organization has been designated to use the proxy method of comparison. It is also important to recognize that there is no limitation period set out in the *Pay Equity Act*, and any wage gaps found to exist can create financial liability to both current and former employees. For this reason, as we enter into a new season of collective bargaining for many organizations, we have provided you with a refresher on the implications of pay equity when at the negotiation table.

Many, if not most, social service sector organizations provide a service in one form or another to members of the public. From time to time, the provision of that service may be subjected to scrutiny under the Ontario *Human Rights Code*, which prohibits discrimination in the provision of services, goods and facilities. While not as common as employment-based discrimination complaints, it is important for organizations to ensure that they are enforcing their respectful workplace and anti-discrimination policies with equal vigour in their dealings with the public in order to avoid raising the spectre of a human rights complaint to the Human Rights Tribunal of Ontario. In this edition, Julia Nanos, an associate in our Toronto office, reviews two recent 2012 decisions from the Human Rights Tribunal that highlight a number of recent issues dealt with by a service provider, including in one case where it was debatable whether any service relationship even existed.

Finally, with an ever-evolving world of technology, the issue of data protection should be first and foremost in the minds of many organizations. Social Service organizations encounter a wide variety of sensitive personal information with respect to the clients they serve. What happens if an employee of the organization loses a file? Or a laptop containing sensitive client information is stolen or lost? Mireille Khoraych, an associate and member of Hicks Morley's Information and Privacy group, provides a useful discussion and helpful tips respecting the limitation of risk and consequences associated with data breaches.

As always, it is our hope that you find the Spring edition of *Reaching Out* informative and useful in your daily human resources operations. If you have ideas for future editions, please do not hesitate to contact me, at lauri-reesor@hicksmorley.com and I look forward to hearing from you.

Lauri A. Reesor
Editor

IN THIS ISSUE

- Pay Equity Considerations During Collective Bargaining
- Service-Based Complaints at theTribunal: Recent Developments
- Data Breaches: Limiting the Risk and Consequences

PAY EQUITY CONSIDERATIONS DURING COLLECTIVE BARGAINING

By: Carolyn Cornford Greaves

In times of fiscal restraint, budget cuts and wage freezes, wage and/or benefit increases achieved during collective bargaining are often are minimal. However, what may seem to be a minimal increase when you are bargaining can quickly become a much larger fiscal commitment for your organization if pay equity considerations are not acknowledged and addressed prior to bargaining. Outlined below are a number of pay equity issues that an organization should consider prior to bargaining to reduce pay equity exposure.

BACKGROUND: THE ONTARIO *PAY EQUITY ACT*

The Ontario *Pay Equity Act* ("Act") came into effect in 1987. The Act requires employers to achieve pay equity and to develop pay equity plans by going through a number of steps, which include:

- Identifying the job classes in the organization;
- Determining the gender dominance of those job classes;
- Gathering job data with respect to the job classes;
- Evaluating the job classes using a gender neutral comparison system;
- Determining job classes of equal or comparable value;
- Identifying the male comparator job class in each band;
- Determining the job rate of the job classes. The job rate is the maximum of the salary range or wage rates and it includes all forms of compensation, benefits and other perquisites;
- Determining whether there are any pay equity adjustments required; and
- Developing a pay equity plan.

Once an organization has achieved pay equity it must be maintained. Pay equity maintenance is triggered in a number of circumstances, including when a new position is created, when a position is eliminated, when there are changes to a position or when there are changes to compensation in an organization.

BEFORE COLLECTIVE BARGAINING – WHAT YOU NEED TO KNOW TO LIMIT YOUR PAY EQUITY EXPOSURE

Collective bargaining can have significant pay equity implications (and as a result fiscal implications) for organizations that have or have not achieved pay equity. For organizations that have achieved pay equity, collective bargaining can affect its efforts to maintain pay equity (particularly if pay equity has not been actively maintained).

For organizations that have not achieved pay equity or where new wage gaps have been created, any wage and/or benefit increases achieved at bargaining may perpetuate and potentially increase any pay equity gaps between female- and male-dominated job classes within the organization, resulting in a larger pay adjustment for the female-dominated job classes in order for the organization to achieve or maintain pay equity.

To limit exposure to potential pay equity liability it is important for an organization to be alive to pay equity considerations prior to bargaining. An organization should know if pay equity has been achieved, what job classes are female-dominated and male-dominated, and which male-dominated job classes are, or may be, male job comparators. Once an organization has this information it should then ask the following questions:

- Will a wage increase as a result of collective bargaining create or perpetuate a pay equity gap?
- Are there male comparators in the bargaining unit that will create pay equity gaps for another employee group?
- Will a wage increase to a specific job class create a pay equity gap?

- Is there a need for “anti-stacking language” to avoid increased pay equity costs?
- Will improvements to other aspects of “compensation” create a pay equity gap?
- What potential arguments and defences can be raised to an interest arbitrator respecting the consideration of pay equity adjustments?

It is important for organizations to know what pay equity gaps exist prior to bargaining so that any increases at bargaining can be allocated towards the closure of these gaps through “anti-stacking” language. It is also important to know which job classes are, or may be, male job comparators because other employee groups will be entitled to any increases (including any additions to benefits) awarded to their male job comparators within the organization (and not just within the bargaining unit). Further, an organization that agrees to lump sum bonus payments or other premiums or allowances for male job comparators without providing the same for female job classes may be in violation of the Act.

Other non-monetary changes at bargaining can also affect an organization’s ability to achieve or maintain pay equity. If additional duties and responsibilities are added to a position or a new job class is created during bargaining, this may result in the need to re-evaluate male job comparators and their placement in a particular points band. It can also impact the pay equity adjustment owed to female job classes.

Ultimately, the more an organization knows about pay equity considerations such as the gender dominance of its job classes, the easier it will be to identify bargaining proposals that could have significant pay equity and financial implications for the organization once bargaining has concluded.

ADDITIONAL CONSIDERATIONS FOR PROXY EMPLOYERS

Organizations in the broader public sector that are subject to the proxy provisions in the Act have additional considerations when going into bargaining. It is important to remember when going into collective bargaining negotiations that organizations subject to the proxy provisions of the Act are required, each year, to expend 1% of the previous years’ payroll towards the achievement of pay equity. Therefore, it is essential for organizations subject to the proxy provisions to be aware that any increase to wages or compensation agreed to during collective bargaining is in addition to the annual 1% obligation. Further, if the negotiated increase is not specifically allocated for pay equity, it may trigger the deeming provision under the Act and affect the organization’s pay equity targets.

Pay equity often presents complex issues for employers with potentially significant monetary implications for organizations. There is no limitation period on retroactive liability and monies may be owed to both current and former employees (plus interest) where pay equity has not been either achieved or maintained.

SERVICE-BASED COMPLAINTS AT THE TRIBUNAL: RECENT DEVELOPMENTS

By: Julia M. Nanos

As many readers will know, the Ontario *Human Rights Code* (“*Code*“) prohibits discrimination in employment on the basis of race, ethnic origin, age, sex, sexual orientation, marital status, disability as well as other protected grounds. Employment-related human rights complaints form the heart of Hicks Morley’s Human Rights practice group. However, many of our clients are engaged in providing services to the public and therefore may face human rights complaints brought by users of their services from time to time. The provision of services, goods and facilities also attract the same *Code* protections.

Two recent cases, both of which were successfully argued by Hicks Morley partner Lauri Reesor, provide useful examples of the type of service complaints service providers may face and offer guidance on the nature of the protections afforded by section 1 of the *Code*, as well as the Tribunal’s jurisdiction with respect to “service”. Though both cases involved claims of discrimination with respect to the provision of education services, the principles are equally applicable with respect to the provision of social services, where organizations are often designed to serve particular interest groups, including persons with

disabilities and other mental health issues.

The decision *Harcourt v. Ryerson University*, [1] involved an allegation by the Applicant that the University failed to accommodate her psychological disability with respect to the provision of its education services. The Applicant had restrictions respecting exam writing which were being accommodated by the University through its Access Centre. In order to arrange for accommodation for any particular exam, the Applicant was required to submit a request for an alternative time/date to her course instructor within one week of the scheduled exam date. The Applicant submitted a request to the Access Centre's online booking system to have her Wednesday evening exam scheduled for Friday based on her personal preferences. However, she did not consult with her professor in advance of doing so, nor did she seek prior approval. On the Monday prior to the scheduled exam, the Applicant's professor received notification of her request to write on Friday. He denied this request for reasons relating to academic integrity; according to University Policy, the Applicant was required to write at the same time as her peers, albeit in the Access Centre. The Applicant took the position that the University failed to accommodate her disability, and she filed an Application with the Tribunal alleging discrimination with respect to the provision of services.

The Tribunal found that, although the Applicant acted reasonably in attempting to have her exam rescheduled, she provided no medical or *Code*-related reason for having to write on Friday. While the Applicant's disability was such that she required certain accommodations (e.g. extended writing time and a quiet environment), section 1 of the *Code* did not entitle the Applicant "to choose the specific time [she] will write an examination on the basis of convenience." Given that the reason proffered by the Applicant for her inability to write on Wednesday related to her work commitments, as opposed to her disability, the University's decision to deny her Friday request was not an act of discrimination.

In sum, the *Code* does not entitle individuals to the accommodation of their choosing, nor will it mandate accommodation where the reasons underlying the request are unrelated to a *Code* ground. The decision reinforces a well-established principle that an individual is not entitled to his or her "preferred" or a "perfect" accommodation but rather, a reasonable accommodation based on the individual's *Code*-related needs. It also highlights the need for service providers to consider first whether the needs of the individual are actually tied to a protected ground under the *Code* as opposed to indicating a preference of the individual. An organization is not required to accommodate where the request is not related to a *Code* protected ground.

Macyshyn v. Ryerson University,[2] provides a variety of useful lessons to service providers. This case involved a 2008 alleged safety and security threat made by the Applicant, who at the time was a former student of the University but who had no current relationship with the University. During a one hour meeting with security officers, the Applicant disclosed he had been to the Centre for Addiction and Mental Health ("CAMH") with respect to his schizophrenia. In his Application with the Tribunal, the Applicant alleged the two officers laughed at him, and made "discriminatory" comments regarding his mental illness. The officers denied making any such comments on the date in question.

The Tribunal concluded that, notwithstanding the Applicant's sincere belief, the statement he recalled being made was, in fact, not made. While the University was successful in this case, the decision is concerning because the Tribunal rendered a decision on the merits without deciding whether it first had jurisdiction. The University had argued that the Tribunal lacked jurisdiction given that the parties were no longer in a "service" relationship and the Applicant had no business to conduct on campus. The Applicant was not a student of the University, nor was the University providing any sort of benefit to him. Under the Tribunal's earlier jurisprudence, "service" was defined as "something which is of benefit that is provided by one person to another or the public." [3] If the Respondent was not providing the Applicant with a "service" as that term is defined by the *Code*, the University submitted the Tribunal did not have jurisdiction to entertain the merits of the Application.

Ultimately, the Tribunal declined to deal with the University's jurisdictional argument and rendered its decision on the merits (albeit in the University's favour). In light of this decision, service providers need to be aware that its interactions with any member of the public may be open to scrutiny even where it is not clear that any service or other business relationship exists. Accordingly, service providers must be cognizant of the need to ensure that all persons with whom it has dealings are treated in a fair and respectful manner, in keeping with the obligations under the *Code*, regardless of whether it is clear a "service" is

in fact being provided.

DATA BREACHES: LIMITING THE RISK AND CONSEQUENCES

By: Mireille Khoraych

In April 2012, Elections Canada lost two unencrypted memory sticks containing the personal information of up to 2.4 million voters, including their full names, home addresses, gender, date of birth and whether they voted in the last election. Typically, such information on memory sticks is password-protected and encrypted, but not in this case. A class action lawsuit was launched in Ontario.

In May 2012, two laptops were stolen from the Elections New Brunswick office. One laptop contained sensitive personal information about every eligible voter in the province, and was password-protected. The data was encoded, and it was linked to a government of New Brunswick domain account, which requires a specific sign-in to access, all in keeping with government policies for information security. The second laptop did not contain any voter data.

In November 2012, Human Resources and Skills Development Canada discovered that a hard drive containing the personal information of some 583,000 Canadians had gone missing. The data included Social Insurance Numbers and birthdates of people who had received student loans between 2002 and 2006. At least three class actions lawsuits have been commenced.

Also in November 2012, Human Resources and Skills Development Canada discovered that a USB key containing personal information, including Social Insurance Numbers, of about 5,000 Canadians was missing.

Incidents of data breach are increasingly making the headlines. It is not clear whether data breaches are actually becoming more common, or whether they are coming to light more frequently due to the increased attention and importance placed on the protection of personal information.

In any case, it is vital that organizations implement, monitor and enforce proper data security measures. This is important not only as an employer vis-à-vis its employees, but also for organizations in the broader public sector, which often hold highly sensitive personal information regarding their clientele.

The case of *Rowlands v. Durham Region Health*[4] provides an example of the potential legal ramifications that can result if proper protection measures are not taken. This was a recent class action in which the representative plaintiff sought damages resulting from the loss of a USB key by a nurse employed by the defendant. The USB key held the unencrypted personal and confidential information of 83,524 individuals who, between October 2009 and December 2009, received HINI immunization shots at a clinic in Durham Region.

The scope of the action was quite broad and included claims for breach of duty of care, breach of fiduciary duty, breach of duty to maintain confidence and privacy to the class member, breach of the *Personal Health Information Protection Act*, breach of section 7 of the *Charter*, and damages for the breach of any of these duties and for the purpose of obtaining credit monitoring or a certain period of time. In addition, punitive relief was sought for aggravated and/or exemplary damages. The action was based primarily on the claim that the confidential information lost could be used to facilitate identify theft.

The action was ultimately settled, which settlement was approved by the Ontario Superior Court in July 2012. The terms of the settlement provided that the defendant would take mitigating steps for class members who could demonstrate that they had suffered economic loss as a result of the data breach, with a claim period up to August 2016. Any such class member who remained unsatisfied with the steps taken could then pursue his or her claim before the Claims Administrators. In approving the settlement, the Court commented that as of the date of the settlement it was “probable that no one has the missing USB key. This inference comes from the fact that no class member has claimed that information on the key has been used to financially damage his or her interests.” In the circumstances, the Court commented that the chances of success of

the class action were quite low.

The personal data on the USB key was described as “minimal” in the settlement decision, even though it included names, addresses, telephone numbers, gender, dates of birth, Ontario health card numbers with expiry dates, names of primary physician and some additional personal health information. An expert witness had provided evidence that more information is usually required to commit fraud, which is sometimes obtained from individuals using the limited information already known about them.

Notably, the settlement also included $500,000 in costs to class counsel, in addition to costs already paid, and a further 25% of any claims paid out in the future.

Although the action eventually settled and it is not clear what damages the Court would have awarded had it found liability on the part of the defendant, this case still serves as a reminder of the potential legal risks associated with data breach.

To mitigate against this occurrence, there are some relatively simple steps that can be taken to limit the risk of significant data breaches occurring in the first instance, and to deal with the consequences of a breach, should one occur. These include the following:

- Personal information on USB keys, portable hard drives and laptops should be encrypted;
- Implementation of a password rule;
- Proper disposal of personal information by shredding; and
- Ensure workplace rules are being followed and enforced, especially those that prohibit the removal of client information from the workplace.

These upfront efforts and costs go a long way towards limiting and mitigating risk down the road. It is therefore advisable that employers undertake regular reviews of their relevant policies and practices, and ensure proper measures are in place and are in fact applied.

Should you have questions or require assistance with any of the issues discussed in this edition of *Reaching Out*, please contact your regular Hicks Morley lawyer.

_____

[1] 2011 HRTO 872 (CanLII).

[2] 2012 HRTO 2331 (CanLII).

[3] *Braithwaite v. Ontario (Attorney General),* 2005 HRTO 31 (CanLII).

[4] 2012 ONSC 3948 (CanLII).
