THE HUMAN RIGHTS TRIBUNAL OF ONTARIO HIGHLIGHTS THE REQUIREMENT FOR CO-OPERATION IN THE ACCOMMODATION PROCESS

Amanda Cohen and Jessica Toldo, Hicks Morley Hamilton Stewart Storie LLP

Municipalities should be aware of a recent decision of the Ontario Human Rights Tribunal that provides support for the proposition that there may be recourse to termination where an employee refuses to co-operate in providing medical documentation. In the recent decision of *Joseph v. Tecumseh Community Development Corporation,* the Tribunal dismissed an application alleging discrimination on the basis of family status and disability, stating that the failure of the Applicant to provide supporting medical documentation to substantiate her absences from the workplace was the reason for her termination.

Background Facts

The Applicant was absent from work from June 2016 until her termination on September 2016. She provided medical documentation to support the first three days of her absence. She then requested and received an additional two weeks off of work to deal with her ailing son and her own health issues. There was also time off for a three-week vacation that had been approved prior to the start of her absences.

On August 3, 2016 the Respondent contacted the Applicant requesting her outstanding medical notes and inquiring as to her return to work plans. No documentation was forthcoming and she did not return to work. On August 11, 2016 the Respondent followed up, again requesting that the Applicant submit details and medical documentation. The Respondent also advised her that if she failed to return to work, or if she continued to not produce the necessary medical information, her position would be considered abandoned. The Applicant responded to this communication asserting that she was "not abandoning her post". However, and despite the Respondent's requests, she did not produce the required medical documentation.

The Respondent continued to ask for medical information from the Applicant to assess her leave of absence request, but the Applicant never submitted this information. As a result of this refusal to co-operate, the Respondent denied the Applicant's request for the leave of absence and terminated her employment on the basis that she had been absent since August 2, 2016 without any authorization.

The Applicant produced the requested medical documentation after she filed her Application with the Tribunal.

The Tribunal Decision

The Applicant alleged that the Respondent employer had discriminated against her on the basis of family status and disability when it terminated her employment.

In dismissing both claims, Vice Chair Patel found that the Applicant had been repeatedly asked for medical documentation, had repeatedly promised to provide it, and had repeatedly failed to do so. The Vice Chair also noted that the Applicant could not, in trying to establish discrimination under the *Human Rights Code* ("*Code*"), rely on her after-the-fact evidence about her family status responsibilities and her health situation which were not known to the Respondents at the time. The Vice Chair concluded that the Applicant's family status, her disability, and her assertion of her rights under the *Code* were not factors in the decision to terminate her employment.

Vice Chair Patel pointed out that the Applicant was "entrenched" in her position about her rights under the *Code* and that she did not have to report to the Respondent or comply with their directives because she asserted family status and disability. The Vice Chair found that the Applicant failed to appreciate that accommodation is a two-way process. The Vice Chair noted that the Applicant refused or was unwilling to provide sufficient and timely information to the Respondents and did not demonstrate to the Respondents that her absence was a necessary accommodation because of her health. The Vice Chair concluded by noting that under the *Code,* the Applicant was required to co-operate with the Respondent's efforts to accommodate her by providing sufficient information, which she failed to do.

Key Takeaways for Municipal Employers

This decision provides helpful guidance on the scope and extent of the duty to accommodate. While each case will be different, this is a helpful reminder that the duty to accommodate is a joint responsibility. An employee has a duty to co-operate and participate in the accommodation process. Part of this duty to co-operate is providing an employer with a reasonable amount of information about their restrictions and limitations that will allow an employer to assess whether and how the employee's needs may be accommodated.

Hicks Morley

Amanda Cohen and Jessica Toldo specialize in labour and employment matters facing municipalities. If you have any questions about this or any other employment matter, do not hesitate to contact Amanda at 416-864-7316 or Jessica at 416-864-7529. They may also be reached by email at: amanda-cohen@hicksmorley.com and jessica-toldo@hicksmorley.com.

We wish to thank articling students Ali Fusco and Rachel Counsell for their assistance in the preparation of these articles.

CYBERSECURITY RISKS TO MUNICIPALITIES: A PRIMER ON RANSOMWARE

Daniel Michaluk and Matin Fazelpour, Hicks Morley Hamilton Stewart Storie LLP

Municipalities are increasingly reliant on computer systems to deliver services as efficiently as possible, giving attackers more opportunity to engage in malicious behavior. Methods of attack are constantly evolving and the frequency of attacks has increased at a worrying degree.

One particular attack method has attracted significant attention in recent years. Ransomware is not particularly new, but there has been a proliferation in its use. The New York Times reported that over 40 municipalities in the United States have been hit with ransomware attacks in 2019.

Municipalities are attractive targets for ransomware. This is because they operate a number of services (such as processing permits or issuing tickets) for which they accumulate valuable data that can be resold. Local governments can hold detailed personal information, including financial information, such

as credit card numbers. There are many municipalities, and even if a particular city or town does not have much sensitive data, the perception or possibility that it does may attract an attack. Further, municipalities may struggle to keep pace with technology refresh cycles, which are growing shorter each year.

What is Ransomware?

Ransomware is a form of malicious software that infects a network and encrypts systems and files. The attack may shut down access to key computer systems such as individual files, programs, or even servers and networks. The encryption is usually accompanied by a message demanding payment in exchange for restoring access to the encrypted data. Payment is generally demanded in bitcoin, a decentralized digital currency.

Most ransomware attacks are launched either through direct hacking into a vulnerable system, or through phishing emails that urge municipal employees to click on files or links that then install malware that encrypts systems and files. In a phishing email, the attacker often masquerades as a trusted entity and attempts to trick the recipient of the email into providing login credentials through a file or link.

How Municipalities Can Prepare

Municipalities should review their preparedness for responding to a cybersecurity incident such as a ransomware attack. Municipal data security programs should view ransomware risk as a priority. To do so, a data security program should consider enforcing the least privilege access to data, two-factor authentication, access controls, and an ongoing information security awareness program that promotes strong phishing awareness. Of particular importance to a ransomware threat, is a robust offline data/system backup capability.

Moreover, municipalities should prepare an incident response protocol that provides for timely and decisive decision-making in the event of an attack. It is also important to assess cybersecurity insurance needs and purchase appropriate levels of insurance coverage. Finally, municipalities can pre-retain an incident response coach (and possibly other service providers) who can provide immediate assistance in the event of an incident.

Hicks Morley

Daniel Michaluk and Matin Fazelpour specialize in privacy, cybersecurity preparedness and data security matters facing municipalities. If you have any questions about this or any other privacy matter, do not hesitate to contact Daniel at 416-864-7253 or Matin at 416-864-7213. They may also be reached by email at: daniel-michaluk@hicksmorley.com and matin-fazelpour@hicksmorley.com.

We wish to thank articling students Ali Fusco and Rachel Counsell for their assistance in the preparation of these articles.