Volume 26, Number 5 • May/June 2017

CANADIAN
CORPORATE COUNSEL
A PRACTICAL REFERENCE FOR CORPORATE, MUNICIPAL, AND CROWN COUNSEL

CYBERSECURITY

Ransomware: The Risks are All Too Real

Frank Palmay
Darcy Ammerman
McMillan LLP
Steve McGeown
RootCellar Technologies

Introduction

The Risk – Cyber attacks are considered one of the most serious risks your organisation faces and ransomware is a currently favoured variation (as evidenced by the recent "WannaCry" cyber attack). It involves accessing your system, encrypting all or an important portion of your data and then offering to give you the encryption key for the payment of a modest amount, usually in the form of a cryptocurrency such as bitcoin.

In addition to the risk of not receiving the key once the payment is made, your organisation faces the risk of others similarly exploring your system's vulnerabilities. Your officers and board should be concerned that a ransom attack may be like the canary in the coal mine; an early warning of dangers that might lie ahead. If a later more serious cyber attack takes place, what kind of exposure might the officers and the board face if they just paid the ransom and did nothing more?

So far the authorities have not required that intrusions and ransoms be reported or held that payments of ransom constitute money laundering. If that changes, ransom attacks will take on a whole different level of risk.

WannaCry

In the recent "WannaCry" global attack, a ransomware variant compromised hundreds of thousands of computers in a matter of hours, resulting in the crippling of vast networks. The attack was likely introduced into the victims' networks via traditional malware vectors: phishing e-mails with infected attachments/links and/or exploiting vulnerabilities in outdated browser/plugins when visiting a compromised website and was not considered to be a targeted attack.[1]

Hardening/Bullet-proofing

How do you protect your organisation, your board and your executives from the risks of cyber ransom attacks?

Technical Hardening – There are five main technical considerations of ransomware that create a technology "game changer" apart from the standard data breach exposures that have proliferated very publicly against many organisations over the last 10 years or so:

- *Data Value is no Longer Absolute* – With credit cards or Personal Health Information ("PHI"), there is a dark web market value attached to this kind of information, which provides the motivation to steal it. But in denying access to the data rather than stealing it, the bad actor doesn't need to find specifically valuable information, they only need to find information YOU might value.

In This Issue

Ransomware: The Risks are All Too Real 65
Overhaul of Alberta's Workplace Laws Now Underway 68
Procedures and Strategies for Anti-counterfeiting: Canada 71
Selecting Candidates – Medical Aspects & Detection Tests 75
Recent Cases 78

- *No Exfiltration/Fencing Requirement* – Part of the bad actors' ROI on malicious cyber-crime typically involves finding a suitable dark market to sell the stolen information, knowing in such an environment they face getting ripped off themselves. The simple process of transferring stolen data out of the target victim network (exfiltration) is another point of risk where the bad actor can be detected by more sophisticated organisations. Ransomware requires no exfiltration, and no need to sell anything to derive value from the successful breach.
- *Attack Vectors are Typically Common Vulnerabilities/Social Engineering* – Every organisation has data. With such a wider range of targets for ransomware, each with their own self-defined valuable data, organisations previously that did not think of themselves as "targets" are now very exposed and in the crosshairs. Common vulnerabilities and simple email phishing schemes are being used successfully to breach unprepared organisations. What made the "WannaCry" attack so prevalent was its use of a recently patched vulnerability in windows SMBv1[2] that allowed it to spread within a compromised network encrypting every vulnerable host and mapped network drive it could access.
- *Automation Implies Indiscriminate Targeting* – With common vulnerabilities and simple phishing techniques being so successful, bad actors have been able to automate the reconnaissance and infiltration processes. This allows bad actors to attack wide swaths of organisations quite indiscriminately without bias. No organisation can be considered safe.
- *Quality Encryption Works Well for Bad Actors Too* – The types of encryption now available to the public, when implemented correctly, are virtually impossible to break. For both asynchronous (RSA 2048) and synchronous (AES 256) methods typically used, it would take more time than there has existed in the universe to brute force crack with millions of CPUs/GPUs.

When ransomware hits, it is very often too late to do anything technically to mitigate it. Due to the prevalence of the "WannaCry" malware, Microsoft took the unusual step of releasing a patch for EOL versions of windows such as Windows XPiii.[3] However, a patch cannot protect against possible mutations and copycat variations.

Most of the traditional security defenses (firewalls, antivirus, etc.) do virtually nothing to prevent or protect against ransomware. To harden defenses against ransomware, you need to abandon the breach detection mentality that these products emphasise in favour of the more proactive managing of risk to break the bad actor automation cycle, and do so at reasonable costs.

Managing risk means attacking risk holistically across these following four main risk dimensions:

- *Core IT Infrastructure Risk* – The core IT infrastructure (networks, platforms, systems) need to be constantly scanned for vulnerabilities; these vulnerabilities then need to be prioritized and mitigated. This is usually accomplished through patching and configuration error detection. Many ransomware packages continue to exploit old and well-known vulnerabilities.
- *Data & Application Risk* – The most critical applications are often HTTP-based, designed to transmit through the firewall to a mobile app through an API. Bad actors can attack these systems directly, or through a phishing attack gain entry to the network and pivot to critical internal applications. It is critical that key data is therefore prioritized for more frequent and thorough "snapshots" for backup and restore capabilities. Often the only recovery possible after a well-crafted and successful ransomware attack is restoring data made possible through a proactive data risk management program.
- *Process Risk* – Processes help target the most critical assets disproportionately against real world vulnerability exploitability. Whether it's a deliberate "red team" penetration team exercise, or the application of multi-factor authentication on the most critically exposed and/or valuable resources, applying process risk means regularly and proactively applying selected processes designed to probe for real exploitability against IT security policies. Since ransomware relies to some extent on automation, so too must an organisation's defenses rely on process and automation.
- *People Risk* – People risk addresses one of the weakest links that are exploited by most ransomware tool kits, namely fooling employees into inadvertently supplying information or being fooled into the allowing of arbitrary execution of code. Applying social engineering penetration tests, anti-phishing campaigns, and security awareness training are all components of a successful people risk management program.

It is only through a proactive risk management strategy combined across these four risk dimensions can you hope to harden your organisation and prevent the potentially damaging effects of ransomware.

Legal bullet-proofing – Even with the benefit of hindsight, courts do not look for perfection. In assessing whether directors and officers fulfilled their governance duties, courts look at the governance processes and procedures of the organisation. Were they reasonable? Were they followed? If the answer to both is yes, courts will be unlikely to second guess. How do you get there?

The first task is to have a credible assessment of the risk. In the case of cyber-breach and ransomware, the chance of it happening is high; the consequences if it does is more difficult to assess.

Some initial questions that are worth considering are:

- As ransomware involves the unauthorised encryption of data,
  - ❑ Is there data that is more sensitive (customer personal info; intellectual property) that should, therefore, receive more attention and protection?
  - ❑ Where is your data stored? What due diligence/oversight is in place to protect your data that is in the hands of suppliers and outsourced entities? What contractual indemnities and limitations are in place for your data in the hands of third parties?
  - ❑ What backup protocols are in place? Are they robust? Secure?
- Does your organisation have a written protocol for protecting or restoring data? Is it robust enough? Is it being followed?
- Does your organisation have the expertise internally to fashion a data protection plan and to monitor adherence to it?

Because the threat of cyber breach and ransomware is so high and so well publicised, not having a procedure in place that addresses it needlessly exposes the board and the officers of the organisation to liability if the organisation suffers a major loss. Having a procedure in place that is not followed is even more dangerous.

Most modern corporate statutes recognise that commercial activity carries risks and that the directors cannot be expected to have all the answers to address the risks. Most statutes, therefore, provide a safe harbour for directors who in good faith rely on the advice of experts. In the case of the *Canada Business Corporations Act*, the relevant provision is:

> A director ... has complied with his or her duties under subsection 122(2) [the duty of care, diligence and skill], if the director exercised the care, diligence and skill that a reasonably prudent person would have exercised in comparable circumstances, **including reliance in good faith on ... a report of a person whose profession lends credibility to a statement made by the professional person.**
>
> A director has complied with his or her duties under subsection 122(1) [fiduciary duty] **if the director relied in good faith on ... a report of a person whose profession lends credibility to a statement made by the professional person.**[4] [emphasis added]

In the area of cybersecurity, one possible way in which a board and in some cases the officers can protect themselves is to have a suitably qualified professional draft or critique the security procedures and then ensure that they are followed.

Risk Transfer – Depending on how and where the cyber attack originated, it might be that another person can be held liable for the damages. For example, if the vulnerability was the result of a failure on the part of a person to which tasks were outsourced, the outsourcing agreement might transfer the liabilities to that person via covenants and/or indemnities. The problems associated with relying only on this are limitations, difficulties of enforcement and the creditworthiness of the person.

Insurance – Inevitably, no matter how robust the cybersecurity processes and procedures are, there will always remain some residual risk. Even if your organization has a "bullet-proof" set of systems and processes protecting it from third party attacks, it is likely that you won't be able to fully account for human error and/or the possible naivety, selfishness or political whims of employees.

The value of a cybersecurity insurance policy to mitigate and protect your organization from this residual risk cannot be overstated. However, cybersecurity insurance is still in its infancy and is constantly evolving. While underwriters continue to struggle with the predictive accuracy of how a cyber breach can impact the business, reputation, property, etc. of organizations of different sizes and complexities across various different sectors, cybersecurity policy coverages, exclusions, deductibles and premiums also continue to change.

Although most claims are currently being made from the health sector where the protection of PHI reigns paramount, the number of claims being made throughout all sectors continues to rise.[5]

Given the relative complexity and interoperability between insurance policies governing cyber, business interruption, property, etc. it is incumbent to work directly with your broker and/or legal counsel to ensure that every breach scenario is contemplated such that the policies in place will cover and adequately respond to a cyber breach (which may or may not have cascading effects).

One area of interest specifically related to ransomware is the balance between paying a ransom (which is often below the deductible, at least for a mid to large size organisation) or going ahead with a claim under your policy. Unfortunately, bad actors have honed in on this limitation and are using it to their advantage. Indeed, most ransomware attackers ask for a relatively small

amount of money (typically below $10,000) such that organizations are more willing to pay the ransom and be done with it. In the area of ransomware, it's really not how big the fish is, but rather how often it bites.

Conclusion

Cybersecurity and ransomware are risks that all organizations must be cognizant of and develop procedures to guard against. Every organization of every size in every country is a target for ransomware. The "WannaCry" malware certainly won't be the last to indiscriminately threaten an organizations' critical IT and data assets.

There are a number of technical, educational, legal and risk transfer factors that should be considered. Since the solutions are interdisciplinary, your organization's IT, risk management and legal advisers should be involved. They can not only reduce the risk of a successful attack, they can help mitigate the legal exposure if you are attacked.

Frank Palmay is a partner in McMillan LLP's Toronto office, where his practice consists of general corporate and commercial law with particular emphasis on insurance matters, health, technology and mining exploration. He is the Co-Chair, Financial Services Regulatory and Cybersecurity. He can be reached at (416) 307-4037 or frank.palmay@mcmillan.ca. Steve McGeown is a 25 year industry veteran of the TCP/IP networking product and IT security services space. He currently holds the position of SVP of Marketing and Products at RootCellar Technologies, a company offering an innovative and new Risk Management-as-a-Service concept. He can be reached at (519) 497-9822 or steve.mcgeown@rootcellartech.com. Darcy Ammerman is a Senior Associate in McMillan LLP's Ottawa office, where her insurance practice focuses on policy review, including cybersecurity, in conjunction with a more general practice advising on all aspects of compliance and legal risk management for federally regulated entities. She can be reached at (613) 691-6131 or darcy.ammerman@mcmillan.ca.

1 RootCellar Technologies, *Frequently Asked Questions: "WannaCry" and Ransomware* (May 15, 2017).

2 <https://technet.microsoft.com/library/security/MS17-010>.

3 <https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>.

4 *Canada Business Corporations Act*, R.S.C. 1985, c. C-44, s. 123 Similar provisions are contained in a number of jurisdictions, including: (1) Ontario *Business Corporations Act*, R.S.O. 1990, c. B.16, s. 135; (2) Alberta *Business Corporations Act*, R.S.A. 2000, c. B-9, s. 123; (3) British Columbia *Business Corporations Act*, S.B.C. 2002, c. 57, s. 157; (4) Manitoba *The Corporations Act*, R.S.M. 1987, c. C225 (C.C.S.M., c. C225), s. 118; (5) Quebec *Business Corporations Act*, C.Q.L.R., c. S-31.1, s. 121; (6) *Bank Act*, S.C. 1991, c. 46, s. 211; and (7) *Insurance Companies Act*, S.C. 1991, c. 47, s. 220.

5 See, for instance, The Canadian Chamber of Commerce, *Cyber Security in Canada: Practical Solutions to a Growing Problem* (April 2017).

EMPLOYMENT LAW

Overhaul of Alberta's Workplace Laws Now Underway

Birch Miller
Bruce Graham
Blake, Cassels & Graydon LLP

Significant changes to Alberta's workplace laws are coming. On May 24, 2017, the Alberta government introduced Bill 17, the *Fair and Family-friendly Workplaces Act* (Bill 17), which proposes the biggest changes to Alberta's *Employment Standards Code*[1] ("Employment Standards") and *Labour Relations Code*[2] ("Labour Code") in decades. It will affect all provincially regulated employers and most of the amendments are expected to be passed into law on January 1, 2018.

Some of the proposed changes, including the banking of overtime at increased rates and a flurry of new measures to promote, enhance and strengthen union activity in Alberta, may be controversial. The provincial government is likely to emphasize fairness and families as the debate surrounding Bill 17 unfolds, since a number of the proposed changes may be perceived as less favourable to Alberta employers. The most noteworthy changes are summarized below.

Employment Standards

Leaves of Absence

A number of new unpaid leaves will be created for the following situations:

- Long-term illness and injury (up to 16 weeks per year)
- Personal and family responsibility (up to five days per year)
- Bereavement (up to three days per year)
- Domestic violence (up to 10 days per year)

- Citizenship ceremony (half-day to attend a citizenship ceremony)
- Critical illness of a child (up to 36 weeks)
- Death or disappearance of a child (up to 52 weeks where the child disappears as a result of a crime or up to 104 weeks if the child dies as a result of a crime)

Bill 17 also modifies and expands many of the leaves that are already in place:
Compassionate Care:

- Extended from eight to 27 weeks
- Caregiver status to include non-primary caregivers
- Notice to return to work reduced to 48 hours from two weeks

Maternity and parental leave:

- Maternity leave extended from 15 to 16 weeks
- Parental leave remains at 37 weeks, but may be increased in the future

Notably, employees will be eligible for current and new leaves after just 90 days of employment (rather than one year as is presently the case). Many of these changes are being made in order to align with federal employment insurance benefits.

Overtime, Compressed Work Weeks and Rest Periods

Overtime agreements will allow for time to be banked for six months (instead of three months). Moreover, the calculation of overtime banking will be expanded from a ratio of 1:1 to 1:1.5. As a result, employers will be required to grant 1.5 hours off for each hour of overtime worked. Such a change does away with the advantage offered to employers by the banking of overtime (employers were previously able to offer one hour for every overtime hour worked rather than paying overtime pay equal to 1.5 time wages).
Compressed work week arrangements (allowing for more working hours in a day at the employee's regular wage over a compressed period) will be renamed "averaging agreements" and will now require the support of the majority of affected employees (or be part of a collective agreement).
Employers will also be required to provide employees a minimum 30-minute break for every five hours of consecutive work (rather than a 30-minute break during each shift in excess of five consecutive hours of work).

Terminations and Temporary Layoffs

Employers will be prohibited from requiring employees to use vacation or banked overtime during the notice of termination period unless otherwise agreed to.

Bill 17 will also impose relatively onerous requirements on employers to notify the minister of labour of group terminations at a single location within a four-week period. Presently, employers are required to provide four weeks' written notice. That notice requirement will now increase by an amount that depends on the number of employees being terminated: eight weeks' notice for 50-99 employees; 12 weeks' notice for 100-299 employees; and 16 weeks' notice for 300 or more employees. Not only does this require employers to be more diligent, it also increases the likelihood of diminished productivity since workers will have a much longer "heads up" that their employment will be terminated.
Temporary layoffs that exceed 60 days (in total) within a 120-day period will amount to termination of employment, unless otherwise agreed to between the employer and the worker (*i.e.*, the employee has agreed to the payment of wages and/or benefits during the temporary layoff period).

Statutory Holiday Pay

Aside from clarifying how holiday pay is to be calculated, Bill 17 also grants eligibility for statutory holiday pay to all employees (*i.e.*, workers no longer need to be employed for 30 days in order to be eligible for statutory holidays).

Youth Employment

A number of changes are also being considered with respect to youth employment, including elevating the minimum working age from 12 to 13. The government also intends to create a list of allowable "light work" that youth under 16 can do (*i.e.*, accommodation and food services). Employing youth in a job not on the list will require a permit. The government is also contemplating the establishment of a list of "hazardous work" and prohibiting youth under 16 from working in jobs on that list (16 and 17-year-olds can only do hazardous work with a permit).

Enforcement and Administration

Bill 17 would also create a new administrative penalty system to fine employers who contravene Employment Standards. In addition, it would extend the period in which the government could bring a prosecution against an employer from one to two years.
Appeals will no longer be heard by umpires (provincial court judges) but instead by members of the Labour Relations Board ("Board").

Farm and Ranch Workers

Farm and ranch workers (except for family members) will no longer be entirely exempt from Employment Standards.

Labour Code

Unsurprisingly, the proposed changes to the Labour Code are geared towards enhancing union powers and

increasing union involvement in Alberta. Some of the most notable changes include the following:

Card Checks and Union Certification

Bill 17 proposes that Alberta adopt a hybrid card-check system in order to certify new trade unions. This is likely to have significant ramifications for union organization in Alberta. Where a union has 65 per cent or more support (as shown by workers signing cards or being members in good standing), the union can become the certified bargaining agent without a secret ballot vote taking place. If between 40 and 65 per cent of employees sign cards, then a secret ballot vote will be conducted. Where union support is shown by way of a petition, a vote will be required.

Most unions in Canada support card-check systems because secret ballots are less likely to result in union representation. The move to a card-check system (even a hybrid one) could escalate unionization in Alberta. Card checks also have the potential to create difficult working environments as union organizers and workers wanting union representation may influence their colleagues to sign cards. Another issue under the card-check system is that employers are less likely to be aware of union campaigns while they are taking place. As a result, unions tend to be the single or dominant source of information and workers may not always be given a balanced picture before electing to support a union.

Bill 17 will also extend the allowable period for union campaigns from 90 days to six months. As a result, unions can now apply for certification long after employees have applied for membership. During the period between an employee signing a card and the union applying for certification, it is possible that employees will change their mind about unionization but, as a result of moving to this hybrid card-check system, they may not have the chance to cast their vote through a secret ballot.

Firm timelines are also being imposed to ensure that certifications are dealt with promptly (20 days from the date of application or 25 days in situations involving a mail-in ballot).

First Contract Arbitration

First contract arbitration will now be available to employers and unions upon application to the Board. This will allow a union to have a first collective agreement imposed on an employer if the union is unsuccessful in bargaining over the course of 90 days. The Board will also have new, wide-ranging powers to direct the parties on next steps (*i.e.*, tabling of final proposals, mediation, ordering votes). Failing a satisfactory outcome, the Board will also be empowered to require binding arbitration of a first collective agreement.

Rand Formula

The inclusion of a Rand formula in collective agreements mandates that dues be deducted from employee pay and remitted to the union. Currently the inclusion of such a clause is negotiated by the parties during bargaining. However, it will now be imposed in all collective agreements upon a union's request.

Unfair Labour Practices

Employers will now have the onus of disproving that an unfair labour practice occurred rather than an employee being required to prove that such conduct occurred. The introduction of this reverse onus provision will make it easier for employees to challenge employer actions such as discipline or dismissal.

The Board will also be empowered to grant a union automatic certification without a vote where an employer is found to have engaged in an unfair labour practice. Similarly, the Board may revoke a union's certificate without a vote where a union is found to have engaged in an unfair labour practice.

Expanding the Labour Code's Reach

Farm and ranch workers (except for family members) will now be able to unionize. Similarly, the definition of "employee" is being expanded to include dependent contractors, which will allow such individuals to collectively bargain with other employees.

Increased Board and Arbitrator Powers

The Board will now have the power to require documentary production in advance of a hearing, deferring disputes where other remedies may be available and prohibiting parties from making the same (or similar) applications. The Board will also be able to order the arbitration of a dispute where it deems an unfair labour practice is occurring.

Union representatives will be granted access to an employer's worksite for the purposes of organizing or carrying out union business, where the Board requires it.

Significantly, arbitrators will be able to extend the time available to grieve a matter even if the time to do so has expired under the applicable collective agreement. Arbitrators will also be given a broad range of powers to expedite proceedings, make interim orders and resolve disputes.

Other notable changes include:

- Unions will have the explicit right to picket the secondary premises of an employer as well as locations of third parties helping an employer resist a strike
- The Board will no longer be able to suspend the deduction and remittance of union dues when an illegal strike is taking place
- Essential services will be expanded to include health care laboratories, blood supply services and

continuing care facilities (including those that are non-profit and privately owned)

- Construction workers no longer need to be employed for 30 days before participating in a union certification vote
- Appeals from arbitration decisions will be heard by the Board (not the courts) and appeals from Board decisions will proceed directly to the Court of Appeal

Conclusion

Few changes to Bill 17 are expected given the government's majority in the legislature. As a result, employers will soon face many new challenges, including compliance and administrative issues, as well as broader strategic considerations.

Birch Miller is a Partner in the Calgary office of Blake, Cassels & Graydon LLP, where she practices in the areas of employment and privacy law. She can be reached at (403) 260-9613 or birch.miller@blakes.com. Bruce Graham is an Associate in the Calgary office of Blake, Cassels & Graydon LLP, where he practises in all areas of employment and labour law. He can be reached at (403) 260-9677 or bruce.graham@blakes.com.

[1] *Employment Standards Code*, R.S.A. 2000, c. E-9.
[2] *Labour Relations Act*, R.S.A. 2000, c. L-1.

INTELLECUTAL PROPERTY

Procedures and Strategies for Anti-counterfeiting: Canada*

Lorne M. Lipkus
Georgina Starkman Danzig
David S. Lipkus
Kestenberg Siegal Lipkus LLP

Legal Framework

Fighting counterfeiting in Canada involves the following legislation:

- the *Trade-marks Act*;[1]
- the *Copyright Act*;[2] and
- the *Criminal Code*.[3]

CETA

On October 30, 2016 Canada and the European Union signed the Comprehensive Economic and Trade Agreement ("CETA") and Bill C-30 (the domestic implementation legislation) was introduced the following day. Ratification is expected in the near future. CETA brings significant changes to Canada's trade-mark and patent laws. Noteworthy are changes relating to the protection of geographical indications. They will be expanded from wines and spirits to include agricultural products and food. They will not be able to be used (as a trade-mark or otherwise) if the product is not produced under the rules of or do not originate from that region. Use of a protected geographical indication on any products that are in the same category as the geographical indication will be prohibited and will be unregisterable. Requests for assistance and importation and exportation prohibitions will be available for protected geographical indications.

Update on Border Enforcement

Although no official statistics have been released, since the border enforcement regime came into force on January 1, 2015, fewer than 200 rights holders have filed their rights with Customs and only approximately 50 shipments have been detained. Unfortunately, several of these shipments were very small quantities of counterfeit merchandise, making it cost prohibitive for the rights holder to sue the importer or take other potential enforcement steps.

Trans-Pacific Partnership Agreement: In-transit Information Sharing

In January 2017 the United States withdrew from the Trans-Pacific Partnership ("TPP") Agreement. In the circumstances, Canada's soft commitment to notify the United States if it identifies goods suspected of infringing copyrights or trade-marks destined for signatory countries – which was to commence on entry into force of the TPP Agreement – may never come to fruition. In a letter from the Canadian government to the US government, Canada expressed a commitment to notify the United States when it identifies goods that, if destined for the United States, would be suspected of infringing copyright or trade-marks (one of the options in the TPP Agreement).

Border Measures

Customs has *ex officio* powers to detain suspected shipments of counterfeit products. Rights holders can

file a request for assistance that is valid for two years. Rights holders can deposit copyright or trade-mark particulars with Customs. This will enable Customs to provide them with notice and enable rights holders to pursue a civil remedy in court.

If a request for assistance is filed, Customs is empowered to detain goods suspected to infringe copyrights or trade-marks, and share information with rights holders to give them an opportunity to pursue a remedy in court. Detention by Customs cannot exceed 10 working days (subject to a further 10 working days (five for perishable goods) upon request of the rights holder). If the goods are counterfeit, the rights holder must use this detention period to commence proceedings in court against the importer and seek an order for seizure and destruction of the counterfeit merchandise. The rights holder is responsible for any applicable storage, handling and destruction charges of any detained goods. Customs has no authority to seize or destroy counterfeit merchandise on its own. Permitted disclosure by Customs to the rights holder includes providing a "sample of the goods" and "information about the goods that could assist them in pursuing a remedy". Limitations restrict the use of that information for any purpose other than to determine whether the import or export of the goods is an infringement or to pursue civil proceedings in court or for the purpose of reaching an out-of-court settlement.

If the rights holder commences proceedings, substantive remedies – both equitable and statutory – are available under the *Trade-marks Act* and the *Copyright Act*, including declaratory relief, injunctive relief, mandatory relief (*i.e.*, forfeiture, destruction) damages and costs. Statutory damages are available only under the *Copyright Act*.

The framework for how Customs deals with counterfeit trade-mark goods or pirated copyright goods is set out in the D-Memorandum (D-19-4-3). Paragraph 18 thereof compels the rights holder to respond to Customs within three business days of first contact by Customs and state whether it intends to pursue a remedy. This creates a three-day pre-notice and a subsequent 10-day notice regime (the former of which was not contemplated by the legislation). Within that three-day pre-notice period, and at the discretion of Customs, no information is provided about the owner, importer, exporter and/or consignee – only pictures and quantities of the suspect shipment are disclosed.

Notwithstanding that the legislation permits Customs to exercise discretion when contacting registered rights holders to initiate inquiries as to the authenticity of goods at the border, in practice, Customs does not exercise that discretion unless the registered rights holder has filed a request for assistance.

Enforcement in Practice

The first two test cases involving this legislation resulted in forfeiture and the destruction of the counterfeit merchandise at the importer's expense. One was resolved within 20 days (10-day detention plus a 10-day approved extension) and the rights holder was not required to sue the importer as contemplated by the legislation. The importer in that case agreed to facilitate the pick-up and destruction of the counterfeit merchandise by the rights holder's agent, from Customs at the importer's own expense, a position that was negotiated by counsel for the rights holder and the importer. In the context of those negotiations, previous imports of similar counterfeit goods already in the country were identified and subsumed within the resolution detailed above.

In the second test case, the rights holder and the importer were unable to resolve the matter within the detention period and the rights holder sued the importer in the Federal Court. A resolution was reached requiring the importer to pay the costs of the bonded storage, bonded cartage and destruction witnessed by Customs. The process was expensive because the goods were "pre-declared" and only the importer (short of a court order) could authorise how the goods could or would be dealt with. The shipment included branded goods, believed to infringe the rights of other rights holders, which had not filed a request for assistance. Accordingly, rights holders that had not filed a request for assistance were not contacted by Customs and their goods were segregated and released to the importer once it paid the duty.

In addition to the abovementioned case, an action has been commenced against an importer of allegedly counterfeit phone packaging, stickers, labels and manufacturing equipment that were presumably to be used to assemble counterfeit products in Canada, thus highlighting to Customs that components and packaging used to manufacture or assemble counterfeit goods are being imported and vigilance in inspection and detention is critical to combat this.

Criminal Prosecution

Product counterfeiting typically involves a violation of trade-mark rights or copyright.

The *Combating Counterfeit Products Act*[4] has created a new offence provision in the *Trade-marks Act*, which states:

> *51.01(1) Every person commits an offence who sells or offers for sale, or distributes on a commercial scale any goods in association with a trade-mark if that sale or distribution is or would be contrary to section 19 or 20 and that person knows that;*

(a) The trade-mark is identical to or cannot be distinguished in its essential aspects from a trade-mark registered for such goods; and

(b) The owner of that registered trade-mark has not consented to the sale, offering for sale or distribution of the goods in association with the trade-mark.

The offence, on a substantially similar basis, extends to the manufacture, possession, import, export or attempted export of goods and labels on a commercial scale; and to the advertisement of service in association with a trade-mark, all without the owner's consent.

Criminal prosecutions in Canada require proof, beyond reasonable doubt, of the act itself (*actus reus*) and subjective knowledge (*mens rea*) of the prohibited act to secure a conviction.

Courts have found that *mens rea* can be proved by circumstantial evidence, such as prior civil lawsuits or judgments of infringement or possession of previously delivered cease and desist letters from rights holders.

The *Copyright Act* provides for penalties for infringement (section 42(1)), including fines of up to C$1 million, imprisonment for up to five years or both. *Criminal Code* provisions on fraud, passing off or forgery involving a trade-mark include fines of up to C$10,000 and/or imprisonment for up to two years.

Although imprisonment is an available punishment for copyright or trade-mark offences, courts and prosecutors rarely impose or recommend jail time. The fines imposed tend to be at the low end of the spectrum.

When imposing penalties for copyright or trade-mark offences, courts apply statutory principles of sentencing:

> *The fundamental purpose of sentencing is to contribute, along with crime prevention initiatives, to respect for the law and the maintenance of a just, peaceful and safe society by imposing just sanctions that have one or more of the following objectives:*
>
> *(a) to denounce unlawful conduct;*
>
> *(b) to deter the offender and other persons from committing offences;*
>
> *(c) to separate offenders from society, where necessary;*
>
> *(d) to assist in rehabilitating offenders;*
>
> *(e) to provide reparations for harm done to victims or to the community; and*
>
> *(f) to promote a sense of responsibility in offenders, and acknowledgment of the harm done to victims and to the community.*[5]
>
> . . .
>
> *A sentence must be proportionate to the gravity of the offence and the degree of responsibility of the offender.*[6]

Canada Consumer Product Safety Act

The *Canada Consumer Product Safety Act*[7] prohibits the manufacture, import, sale or advertisement of consumer products that could pose an unreasonable danger to the health or safety of Canadians. Other prohibitions relate to the packaging, labelling or advertisement of a consumer product in a manner that is false, misleading or deceptive in respect of its safety. For example, the unauthorised use of certification marks is prohibited. The prohibitions and powers in the Act may prove to be useful tools in the fight against counterfeit consumer products, provided that the consumer product poses a danger to human health or safety.

Civil Enforcement

Civil remedies are the most commonly employed means to address counterfeiting issues. The framework for civil actions is primarily statutory – the *Trade-marks Act* and the *Copyright Act*. While there are common law prohibitions against the passing off of registered or unregistered trade-marks, section 7 of the *Trade-marks Act* embodies the substance of common law passing off and is most frequently used. Actions commenced for infringement under these statutes may be brought in a provincial court or in the Federal Court. The applicable statutes include the following remedies:

- injunctions;
- preservation orders;
- damages;
- accounting of profits;
- destruction of infringing goods;
- punitive damages; and
- recovery of a portion of legal costs.

The *Combating Counterfeit Products Act* amended the *Trade-marks Act* to expand the rights conferred by registration to include the right to preclude others from manufacturing, possessing, importing, exporting or attempting to export any goods, labels or packaging for the purpose of their sale or distribution if:

- they are identical or confusingly similar to a trade-mark registered for such goods;
- the owner of that registered trade-mark has not consented to have the goods, labels or packaging bear the trade-mark; and
- the sale or distribution of the goods would be contrary to the *Trade-marks Act*.

Under the *Trade-marks Act*, damages and accounting for profits are alternative remedies. Under the *Copyright Act*,

both damages and disgorgement of the infringer's profits are recoverable. It also provides the option of electing statutory damages per copyright infringed, while the *Trade-marks Act* lacks statutory damage provisions.

The *Federal Courts Rules*[8] expressly provide for the preservation of the subject matter of litigation. Typically, motions for preservation are brought on notice to the alleged infringer and, if successful, an order is issued requiring the alleged infringer to deliver up the subject merchandise pending the final outcome of the lawsuit.

An Anton Piller order (typically granted *ex parte*) orders the party served to deliver up the goods alleged to be counterfeit for preservation pending determination of the lawsuit. While refusal potentially subjects a party to contempt of court proceedings, compliance is nevertheless voluntary and parties executing Anton Piller orders cannot breach the peace if the party served refuses to cooperate. An independent supervising solicitor, who does not represent the rights holder, supervises execution of Anton Piller orders and must fully explain the terms of the order, supervise any permitted searches of the subject premises and ensure that any potential privileged documents are preserved in a manner that allows the party served to assert privilege before they are disclosed. Law enforcement typically attends to keep the peace and to assure the party served that the process is legitimate.

Canadian courts have issued rolling Anton Piller orders in John Doe/Jane Doe actions, in which the identities of the infringers are not yet ascertained. Following execution of a rolling Anton Piller order, the courts have an established mechanism for reviewing execution of the service and adding the party served as a named party defendant.

Civil remedies for trade-mark and copyright infringement have the potential for greater damages than have been awarded as fines in the criminal context. However, where counterfeiters fail to keep business records, ascertaining appropriate damages or quantification of profits is difficult. In such circumstances, the Federal Court has established minimum compensatory damage awards for trade-mark counterfeiting. Where no documents are delivered up by the defendant to quantify sales, profits and/or damages, the court regularly awards damages to successful litigants using a defined scale of damages, depending on the nature of the business (itinerant vendor, fixed retail and wholesaler/importer). Minimum compensatory damages have been awarded on a per instance of infringement basis or on a per inventory turnover basis.

Anti-counterfeiting Online

The *Copyright Act*:

- prohibits circumvention of technological protection measures (section 41.1);
- prohibits the manufacture, import and sale of technologies, devices and services designed primarily for the purpose of breaking digital locks (section 41.1);
- defines "infringement" to include services that primarily enable acts of copyright infringement by means of the Internet or other digital networks (enumerating the factors to consider); and
- sets statutory damages (C$500 to C$20,000 for commercial infringements and C$100 to C$5,000 for non-commercial infringements). Proportionality and the infringer's good or bad faith are two of four enumerated factors to be considered (section 38.1).

On January 2, 2015 Canada adopted a "notice and notice" regime which does not require Internet service providers ("ISPs") to take an affirmative step to remove a copyrighted work. ISPs and search engines will be exempt from liability when they act strictly as true intermediaries in communication, caching and/or hosting services. Although Canada is a signatory to the TPP Agreement, given the recent political uncertainty associated with the United States' ratification of the TPP Agreement, the establishment of a notice and takedown regime is uncertain. The *Copyright Act* enumerates exceptions to infringement in respect of the following categories of non-commercial activity:

- Format shift – copying content from one device to another. This provision does not apply to content protected by a digital lock or other technological protection measures (section 29.22).
- Time shift – recording television, radio and Internet broadcasts and listening to or watching them later. This provision does not apply to on-demand/streamed content or content protected by a digital lock or other technological protection measures (section 29.23).
- Mash-up – incorporating legally acquired copyrighted content into user-generated work. This provision is applicable only in the event that the mash-up is not a substitute for the original material, has not been created for commercial gain, and does not have a substantial negative impact on the markets for the copyrighted work or creator's reputation. An example is posting a combination of a Jay-Z rap with a Beatles song on a social networking website, provided that the user-generated work is not subject to the exceptions listed above (section 29.21).

Apart from the *Copyright Act*, Canada has no specific legislation addressing the online sale of counterfeit goods.

Instead, traditional methods are used. For example, copyright owners alleging infringement against unidentified BitTorrent users have advanced motions to compel third-party discovery of the ISP, requesting the handover of subscriber information.

Canadian Anti-fraud Centre

The Canadian Anti-fraud Centre ("CAFC") is jointly managed by the Royal Canadian Mounted Police, the Ontario Provincial Police and the Competition Bureau, and its mandate includes the sale of online counterfeit goods. The CAFC works with payment processors to cancel the counterfeiter's merchant account(s), negating the counterfeiter's ability to process payments, rendering the websites useless. Canadian victims that purchase counterfeit merchandise are encouraged by many rights holders to contact their payment processor and the CAFC in an effort to thwart the illegal sale of counterfeit merchandise in Canada. In 2016 the CAFC received over 18,000 complaints of cyber-related fraud and estimated over $37 million in losses.

Separately, there continues to be an increase in Canadian Internet Registration Authority ("CIRA") domain name dispute resolution policy proceedings, as counterfeiters are hijacking domain names with Canadian extensions in bad faith. A rights holder can file a complaint pursuant to the CIRA Domain Name Dispute Resolution Policy (with either Resolution Canada Inc. or the British Columbia International Commercial Arbitration Centre) against the registrant of a domain name if:

- the rights holder can prove its rights in the trade-mark;
- the registrant has no legitimate interest in the domain name; and
- the domain name was registered in bad faith.

Preventive Measures/Strategies

Canada has no national IP law enforcement coordination body. However, significant lobbying efforts increased this year to remind the Canadian government of the evolution of digital technology and the need for strong cybersecurity. Although two parliamentary committees have recommended that an IP crime taskforce be established as part of legislative reform, such legislation has not yet been enacted. Accordingly, the primary responsibility for battling counterfeit products lies with rights holders, which must take steps to protect and enforce their rights through comprehensive licensing arrangements, diligent civil enforcement and training of and cooperation with law enforcement and customs authorities.

Lorne M. Lipkus is a founding partner at Kestenberg Siegal Lipkus LLP, practising IP litigation with a focus on anti-counterfeiting enforcement, both civilly and criminally, throughout Canada. He can be reached in Toronto at (416) 342-1112 or llipkus@ksllaw.com. Georgina Starkman Danzig is a partner at Kestenberg Siegal Lipkus LLP. She practises IP litigation with a focus on anti-counterfeiting enforcement both civilly and criminally, throughout Canada. She can be reached in Toronto at (416) 342-1108 or gdanzig@ksllaw.com. David S. Lipkus is a partner at Kestenberg Siegal Lipkus LLP, practising civil and commercial litigation with a focus on IP brand protection and insurance defence litigation. He can be reached in Toronto at (416) 342-1103 or dlipkus@ksllaw.com.

---

* This article first appeared in *Anti-Counterfeiting: A Global Guide 2017*, a supplement to *World Trademark Review*, published by Globe Business Media Group – IP Division. For further information please visit <www.worldtrademarkreview.com>.

1 *Trade-marks Act*, R.S.C. 1985, c. T-13.
2 *Copyright Act*, R.S.C. 1985, c. C-42, as amended.
3 *Criminal Code*, R.S.C. 1985, c. C-46.
4 *Combating Counterfeit Products Act*, S.C. 2014, c. 32.
5 *Criminal Code*, s. 718.
6 *Ibid*., s. 718.1.
7 *Canada Consumer Product Safety Act*, S.C. 2010, c. 21.
8 *Federal Courts Rules*, SOR/98-106.

EMPLOYMENT LAW

Selecting Candidates – Medical Aspects and Detection Tests

Éric Latulippe
Francine Legault
Langlois Lawyers LLP

Employers have always sought to implement a selection process for hiring the best candidates for their organizations. This crucial step allows employers to ensure the reliability and physical and mental capabilities of potential employees, who will hopefully provide them with diligent and reliable services, one of the rare obligations incumbent on workers in labour relations matters.

In connection with the selection process, employers will thus want to ensure that this special someone will be able to perform all of his or her duties in a prudent and safe manner, thereby helping the employer meet its obligations to protect the health, safety and security of its workers.

In order to do this, and to satisfy themselves concerning the true capabilities of their future employees, employers have a recognized right, when hiring employees, to verify that they have the normal professional aptitudes required by their positions and the duties inherent therein.

In light of the foregoing, there is no question that an employer has a legitimate right to require that the candidates it has selected for a particular position participate in a selection process that may justify a physical or psychological examination in accordance with certain criteria.

The nature of the operations involved in the employer's business and the duties for which the employer is planning to hire a candidate (its management right) are most definitely criteria according to which the employer may also justify the need to utilize medical tests or questionnaires.

The Legislation

As is the case for all required steps in connection with relations with their active employees, employers have to deal with certain limits on their rights when selecting future employees. Such limits involve privacy rights, how employers must collect, use and retain personal information, and the exercise of discrimination, justified or not, when choosing candidates.

In Quebec, organizations whose activities are governed by federal law are subject in particular to the obligations provided for in the *Canadian Human Rights Act*,[1] the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*.[2]

Organizations under provincial jurisdiction are subject to similar provisions set out in particular in the *Charter of Human Rights and Freedoms*,[3] the *Civil Code of Québec*,[4] the *Act respecting the Protection of Personal Information in the Private Sector*[5] and the *Act respecting Industrial Accidents and Occupational Diseases*.[6]

The Recognized Principles

In the course of the recruitment process, employers have a tendency to collect a great deal of information, which can be of "variable relevance". While some information may be indispensable in deciding whether or not to hire a candidate, the same cannot be said of other kinds of information.

Generally speaking, the courts authorize employers to collect, use and retain only information that is necessary to allow them to confirm that a candidate is capable of performing the specific duties involved in the position he or she is applying for.

The job application form is definitely the tool most relied upon by employers in the recruitment process. Straightforward and easy to use, it can nevertheless give rise to an invasion of privacy or be the basis for discrimination. In order to avoid them being used as ready evidence of an unjustified invasion of a candidate's privacy, such application forms should be prepared in light of the requirements for each specific position to be filled within the organization. By the same token, customizing job application forms is particularly relevant when questions concerning the physical or psychological limitations of a candidate are justified because of the specific requirements of a task or position.

While the objective customizing of a job application form can in most cases be a relatively simple exercise, the same cannot be said about job interviews, which because of their dynamics may prove difficult to control when the time comes to inform the candidate of certain aspects of the employment position being sought. In such situations, a standardized interview form can be useful in ensuring that employers respect the limits of their right to inquire into candidates' personal lives.

When an employer requires a candidate to disclose medical information, it is definitely invading the candidate's privacy. Before imposing such a requirement, the employer must determine whether the line of inquiry is necessary and justified by the specifics of the position in question.

Apart from the fact that a medical questionnaire or examination is an invasion of a candidate's privacy, the decision not to hire a candidate for medical reasons can definitely be characterized as discriminatory. If challenged, the employer will have to show, based on convincing evidence, that:

1. The medical questionnaire or examination is directly and essentially related to determining the candidate's ability to perform the duties inherent in the position;
2. The standard pursuant to which the decision was made was adopted for a rational purpose related to the performance of the work, on the basis of the actual requirements of the position applied for;
3. The standard was adopted in the sincere conviction that it was necessary; and
4. It is impossible to accommodate employees with the same limitations as the candidate without experiencing undue hardship.

Specific Steps

In addition to the limits canvassed above, it should be noted that several decision-making authorities have

already expressed reservations regarding the validity of tests of a psychological nature. Moreover, since psychometric tests are, generally speaking, inherently personal and invasive, in order to justify them the employer must demonstrate, in addition to their reliability, that they are necessary in order to determine the existence of personality traits that are required because of the specific demands of the position.

In another vein, when an employer wishes to include a drug or alcohol detection test as a hiring condition, it must be able to objectively demonstrate the need for doing so, as this too is an invasion of candidates' privacy. In this regard the case law is clear that the employer cannot simply argue that employees who do not consume drugs or alcohol are more efficient, diligent and better performing. This is all the more true since, beyond the purely subjective aspect of such an assertion, the reliability of such detection tests is frequently one of the foremost factors taken into consideration by the courts in rejecting them. To the extent that, for safety and security concerns or in order to assess whether the candidate has the required aptitudes for the position, an employer still wishes to administer such tests, it is essential that it first make a very detailed and specific analysis of the positions and candidates involved in order to demonstrate that they are justified.

Selection by a Sub-contractor

Employers who require candidates to undergo a medical examination frequently, if not generally, retain the services of a firm specialized in this area. While legitimate, the implementation of a selection process in concert with one or more specialized firms raises important issues involving privacy rights and the confidentiality of the personal information so obtained, and the potentially discriminatory decisions that may ensue. There is also the sensitive issue of the liability of those persons taking part in such a process.

In theory, one is not liable for the acts of a co-contractor that harm a third party. However, that is not necessarily the case in labour relations matters, particularly where the implementation of a hiring process is concerned. Despite having retained the services of an independent contractor to assist it, the employer will be solely responsible for the decision whether or not to hire a candidate, and for the consequences of that decision. The employer must ensure that the contractor, as the employer itself is bound to do, limits itself to making only those inquiries and observations that are related to the candidate's ability to perform the duties of the position sought.

Consent

Throughout the selection process, the employer must not only obtain the candidate's express consent to the gathering of information about him or her by the employer, but to the use of that personal information as well. Such consent must of course be free and informed, but in order to be valid it must also be obtained for specific purposes directly related to the decision whether or not to hire the candidate.

Accommodation

Since an employer cannot refuse to hire a candidate for specific medical reasons, except where any associated limitations preclude the candidate from performing the duties of the position applied for, in what circumstances is the employer bound to take measures to accommodate a candidate's limitations?

Where discrimination is concerned, the courts recognize that the employer's obligations, whether at the hiring stage or when the individual concerned is already in its employ, are the same. Thus, when an employer decides to have a candidate undergo a medical examination, it must assume the consequences of that exercise, which may compel it to put in place accommodation measures.

Even if a candidate succeeds in demonstrating that he or she was discriminated against at the hiring stage, the employer may counter by maintaining that its impugned decision or practice was a justifiable business necessity, as it could not have implemented accommodation measures without incurring undue hardship.

To succeed in this regard, the employer must demonstrate that it made reasonable efforts to adjust the requirements of the position sought or to find an alternative position compatible with the candidate's limitations, but was unable to do so without incurring undue hardship.

Conclusions

In our view it would not be prudent for an employer to require a candidate to provide it with medical information if the nature of the duties of the position applied for, or the actual risks posed by one or more of the candidate's medical conditions for the safe performance of those duties, do not justify requiring that information.

If the candidate succeeds in showing that he or she was discriminated against on the basis of a handicap, the court will only order that the candidate be hired if the candidate can establish that he or she would have been hired but for the handicap.

In order to avoid finding yourself in a situation where you are accused of discrimination, or at the very least in order to reduce the risk of that happening, we recommend that you not require the candidate to fill out a medical questionnaire or undergo a medical examination until the very last stage of the hiring process, but in all events before hiring the candidate.

Éric Latulippe is a Partner in the Quebec City office of Langlois Lawyers LLP, where he works primarily as a legal advisor and

attorney in administrative, labour, and occupational health and safety law. He can be reached at (418) 650 7904 or eric.latulippe@langlois.ca. Francine Legault is a Partner in the Montreal office of Langlois Lawyers LLP, where she focuses her practice on occupational health and safety. She can be reached at (514) 282 7848 or francine.legault@langlois.ca.

[1] *Canadian Human Rights Act*, R.S.C. 1985, c. H-6.
[2] *Privacy Act*, R.S.C. 1985, c. P-21.
[3] *Charter of Human Rights and Freedoms*, C.Q.L.R., c. C-12.
[4] *Civil Code of Québec*, C.Q.L.R., c. CCQ-1991.
[5] *An Act respecting the Protection of Personal Information in the Private Sector*, C.Q.L.R., c. P-39.1.
[6] *An Act Respecting Industrial Accidents and Occupational Diseases*, C.Q.L.R., c. A-3.001.

RECENT CASES

Available in PDF – Images of reported decisions (as they appear in the law reports) and original judgments are available as PDF files. To request PDF files, please contact Customer Support at CustomerSupport.LegalTaxCanada@TR.com or 1-800-387-5164 (Toll Free Canada & U.S.).

The summaries below are prepared from material extracted from the All Canada Weekly Summaries (ACWS), and Canadian Labour Arbitration Summaries (CLAS), publications of Canada Law Book.

CLASS ACTIONS

Procedure for material change to wording of common issues is matter of importance to all class actions

Facts: The plaintiff brought a motion for certification of the action as a class proceeding. The motions judge issued an oral ruling granting the certification motion and defining the common issues. There was no transcript and the parties disagreed as to how the common issues had been defined in the oral ruling. When the motions judge eventually released his decision, it was clear that following the hearing the motions judge was not satisfied with the definition of the common issue of breach of standard/duty of care and as a result he had amended or "recast" that portion on his own initiative. The defendant brought a motion for leave to appeal those portions of the order that certified the proceeding as a class action and defined the common issues.

Held: The motion was granted in part. Leave to appeal was granted with respect to that portion of the order setting out the common issue of breach of standard/duty of care. The fairness of the procedure leading to the order certifying the action as a class proceeding was an issue that could be appealed under s. 30(2) of the *Class Proceedings Act, 1992* (Ont.). The correctness of the procedure followed by the motions judge on the motion was open to very serious debate. The question of the procedure to be followed before a material change is made to the wording of the common issue was a matter of importance to class action proceedings generally and was a question of importance that extended beyond the interests of the parties and affected the development of the law in class proceedings litigation more generally.

Levac v. James, 2017 ONSC 2280, 2017 CarswellOnt 5146, 278 A.C.W.S. (3d) 479 (Ont. S.C.J.).

COMPETITION LAW

Indeterminate liability no bar to claim under *Competition Act*

Facts: The plaintiff alleged that the defendant conspired to fix the price of lithium ion battery cells manufactured and sold in Canada, which raised the prices of all lithium ion batteries, including ones purchased from manufacturers who were not co-conspirators. The plaintiff brought a competition law class action on behalf of direct and indirect purchasers in two distribution channels in the marketplace for rechargeable batteries. The motions judge granted the plaintiff's motion to certify the class action. The judge held that the plaintiff had satisfied the cause of action criterion only for the statutory cause of action set out under ss. 36 and 45 of the *Competition Act* (Ont.). The judge did not certify the claim for the umbrella purchasers. There was no relationship, direct or indirect, between the umbrella purchasers and the defendant, apart from the fact that they were trading in the same market. The judge did not certify the claims for unlawful means conspiracy and unjust enrichment. The plaintiff, with leave, appealed the denial of certification of the unlawful means conspiracy claim and the umbrella purchaser claims.

Held: The appeal was allowed in part. The judge erred in denying the certification of the unlawful means conspiracy claim. The Court of Appeal had permitted an amendment to plead an unlawful means conspiracy in a similar case and, on the principle of *stare decisis*, this court was bound to follow that decision. The judge did not err in denying the certification of the umbrella purchaser claims. The judge was right to conclude that allowing claims by umbrella purchasers would expose the defendant to indeterminate liability. There was no reason, however, to exempt a claim under s. 36 of the Act from the application of the principle of indeterminate liability.

Shah v. LG Chem, Ltd., 2017 ONSC 2586, 2017 CarswellOnt 6145, 278 A.C.W.S. (3d) 529 (Ont. Div. Ct.).

CONTRACT LAW

President and company jointly & severally liable for misrepresentation

Facts: The plaintiff designed and built plants for oil and gas field use, the defendant company was the manufacturer of pressure vessels and other industrial equipment, and the individual defendant was the president and directing mind of the company. The parties entered into two contracts that required the company to supply the plaintiff with certain gas plant equipment and pressurized vessels that it required for contracts with third parties for two projects in Pakistan. Both contracts required completion upon timelines set by the plaintiff, and the company was advised that if there was non-compliance with these timelines, then the plaintiff was subject to the forfeiture of performance guarantees provided in its agreements with third parties. Based upon the defendants' representations as to the status of the work, the plaintiff made progress payments to the company on the contracts. The plaintiff alleged that the work was not completed, the product that had been contracted for was not supplied, and the money paid to the company was not refunded. The plaintiff brought an action seeking the return of $422,300 it had paid to the company plus damages equal to the full amount of the performance guarantees that were drawn upon by its third-party customers; the defendants counterclaimed for damages for breach of contract.

Held: The action was allowed and the counterclaim was dismissed. The company had completely failed to perform its contractual undertakings and had caused a fundamental breach of the contracts, and the plaintiff was entitled to have the money it had paid returned to it by the company. The company would not have received the second payment on the first contract but for the fraudulent misrepresentations of the president, and the president was jointly and severally liable with the company for the amount that the plaintiff had paid as the second milestone payment. The purchase orders issued to the company resulted from contracts the plaintiff had entered into with third parties, and the plaintiff was required to issue a performance guarantee for any breach of contract that included a condition for on-time delivery. The plaintiff had made it clear to the defendants that there was a hard, short deadline by which the company was expected to complete its work or there could be penalties incurred by the plaintiff. The plaintiff had met its evidentiary burden to show that the parties had a reasonable understanding that any delay in the completion and delivery of the company's product could result in the execution of performance bonds by the plaintiff's customers, and the plaintiff was entitled to be compensated by the company for its loss of these performance guarantees in the total amount of US$840,480. The president was jointly and severally liable for US$340,265, which was the amount of the performance guarantee the plaintiff had paid under the first contract because the president's false representations delayed the plaintiff from finding out that the company could not perform, leaving the plaintiff unable to fulfil its obligations. The president understood his misrepresentations put the plaintiff at risk of losing its performance guarantee. However, the plaintiff had not established that it was induced by the president's false representations to pay money on the second contract, and the delays causing the third party to execute on the performance guarantee on the second project could not be attributed personally to the president.

Kocken Energy Systems Inc. v. Fulton Engineered Specialities Inc., 2017 NSSC 103, 2017 CarswellNS 273, 278 A.C.W.S. (3d) 539 (N.S. S.C.).

EMPLOYMENT LAW

Employee guilty of wilful misconduct denied termination/ severance pay under ESA

Facts: The employee, 43 years old, had worked for approximately nine years as an automotive technician at a dealership owned by the employer when his employment was terminated. The employee was an experienced automotive technician and was a high earner, but he often rushed work and had been reprimanded on several occasions for poor performance. The employer alleged that that the employee was terminated for cause for allegedly falsely reporting that the brake pads of a car he had inspected had significant wear and had to be replaced. The employee admitted that his measurement of the brake pads was inaccurate, but denied that he had intentionally understated their size or their need for replacement. The employee brought an action seeking damages for wrongful dismissal, termination pay and severance pay under the *Employment Standards Act, 2000* (Ont.).

Held: The action was dismissed. The employee had intentionally misrepresented that the customer's brake pads needed to be replaced, and that constituted wilful misconduct. The employee was not entitled to termination pay or severance pay under the Act because he was guilty of wilful misconduct, disobedience or wilful neglect of duty that was not trivial and was not condoned by the employer.

Cummings v. Quantum Automotive Group Inc., 2017 ONSC 1785, 2017 CarswellOnt 5122, 278 A.C.W.S. (3d) 80 (Ont. S.C.J.).

TRADE-MARKS LAW

Confusion analysis should be limited to earliest material date

Facts: The applicant applied under s. 30 of the *Trade-marks Act* (Can.) to register two trade-marks, BENJAMIN MOORE NATURA and BENJAMIN MOORE NATURA & Design to be used in association with interior and exterior paints. The opponent asserted that the marks were confusing with nine of their trade-marks that included the term "natura". The opponent's oppositions were rejected by the Trade-marks Opposition Board. The opponent appealed the decision and introduced new material evidence on appeal. The Federal Court undertook a *de novo* review of the matter and concluded that there was confusion between the trade-marks, particularly as those marks were used in association with paint. The applicant's applications for registration were refused. The applicant appealed.

Held: The appeal was allowed. The judgment of the Federal Court was set aside and the matter was referred back to the Federal Court for redetermination. The Federal Court did not apply the proper mark-to-mark analysis and take into account the relevant material dates for each ground of opposition. The Federal Court undertook consideration of each of the relevant surrounding circumstance as required by s. 6(5) of the Act; however, the distinctions between the parties' respective marks and the particular material dates were expressed in a very general manner. The Federal Court erred in its confusion analysis by not limiting its consideration to the earliest material date with respect to paints trade-marks. Throughout its confusion analysis, the Federal Court referred to actual sales of paint as a factor to be considered, although neither party was selling paints with these trade-marks at the material date. The Federal Court concluded that consumers would likely be confused as to the source of the paint associated with these trade-marks at least as of the later material dates, but the later material dates were not relevant to the analysis.

Benjamin Moore & Co. v. Home Hardware Stores Ltd., 2017 FCA 53, 2017 CarswellNat 760, 277 A.C.W.S. (3d) 173 (F.C.A.).

Publisher . . . . . .Canada Law Book

Executive editor . . . . . .Sandra B. Kidd, LL.B.

Editor . . . . . .Kayla Rice

Canadian Corporate Counsel is a publication of

THOMSON REUTERS CANADA

One Corporate Plaza
2075 Kennedy Road
Toronto, ON M1T 3V4
1-416-609-3800 (Toronto & International)
1-800-387-5164 (Toll Free Canada & U.S.)
Fax 1-416-298-5082 (Toronto)
Fax 1-877-750-9041 (Toll Free Canada Only)
Email CustomerSupport.LegalTaxCanada@TR.com

Canadian Corporate Counsel welcomes comments and suggestions from its readers. Please address your correspondence to the executive editor.

Canadian Corporate Counsel is published eight times per year and includes an annual cumulative index.

Publications Mail Agreement No. 40064652

ISSN 118-2026 Printed in Canada by Thomson Reuters on recycled paper