# TRANSPORTATION & LOGISTICS GROUP NEWSLETTER

September 2023

In the September issue:


## Bill C-47 Increases Limits of Liability for Marine Accidents

Page 2

By Rui M. Fernandes

## Forced or Compulsory Labour Laws in Canada

Page 2

By Rui M. Fernandes

## Mitigating Cyber Risk in the Trucking Sector

Page 8

By Jamal Rehman

## Changes to Termination Notice Period for Interprovincial and Cross-Border Trucking Companies as of February 1, 2024

Page 10

By Saisha Mahil


Founded in the 1920s, Gardiner Roberts LLP has grown to become a strategically placed mid-sized business law firm with a diverse client base which includes several of Canada's largest banks, public companies including mining, high tech and software companies, real estate enterprises, lenders and investors.


**Rui M. Fernandes**
Partner
416.203.9505
rfernandes@grllp.com

**Kim E. Stoll**
Partner
416.203.9509
kstoll@grllp.com

**Jamal Rehman**
Associate
416.203.9819
jrehman@grllp.com

**Saisha Mahil**
Associate
416.203.9547
smahil@grllp.com

# Bill C-47 Increases Limits of Liability for Marine Accidents

By Rui M. Fernandes

On June 22nd, 2023 Bill C-47 received Royal Assent. The legislation entitled "*An Act to implement certain provisions of the budget tabled in Parliament on March 28, 2023*" S.C. 2023 c. 26 contains provisions that came into force on June 22nd 2023 relating to the limits of liability for marine accidents.

Transport Canada has advised that the bill implements changes to the *Marine Liability Act*. A summary of the changes are as follows:

(a) increases the maximum liability for certain claims involving a ship of less than 300 gross tonnage from $1 million for loss of life and personal injury and $500,000 for any other claims to $1.5 million and $750,000, respectively;

(b) establishes the maximum liability for claims involving air cushion vehicles using the limits in the LLMC (The Convention on Limitation of Liability for Maritime Claims, 1976);

(c) applying Part 4 of the *Marine Liability Act* to air-cushion vehicles, making them strictly liable for damage suffered as a result of the death of or personal injury to a passenger;

(d) extending the application of the International Convention on Civil Liability for Bunker Oil Pollution Damage, 2001 to non-seagoing vessels;

(e) clarifying that the owner of a ship is liable for economic loss related to fishing, hunting, trapping or harvesting suffered by an Indigenous group, community or people or suffered by a member of such a group, community or people;

(f) providing for a modernized public notice requirement relating to the constitution of limitation funds;

(g) allowing the amount of a limitation fund to be reduced if the shipowner has paid out claims related to an oil spill before the limitation fund is created; and

(h) expanding the compensation regime of the Ship-source Oil Pollution Fund to include certain future losses (losses that have not yet occurred but will almost certainly occur).

Of significant importance to pleasure craft owners and insurance brokers and insurers are the increased limitation of liability amounts. A typical insurance policy issued prior to the legislation coming into force provided for $2 million of coverage. This was to protect the boat owner/operator for an event that had a loss involving personal injury and property damage. One million was the limitation of liability for personal injury losses and $500,000 for property damage for a total of $1,500,000. With interest and court costs a policy of $2 million would suffice. With the increased limits to $1,500,000 for personal injury and $750,000 for property damage, the needed coverage would be $2,250,000.00. When interest and costs are added, boat owners should get $3 million of coverage.

# Forced or Compulsory Labour Laws in Canada

By Rui M. Fernandes

### *Introduction*

On May 11th, 2023 Bill S-211 *An Act to enact the Fighting Against Forced Labour and Child*

*Labour in Supply Chains Act and to amend the Customs Tariff*" received Royal Assent. The legislation will come into force on January 1st, 2024. The first reports under the legislation are due May 31, 2024.

The purpose of the *Act* is to implement Canada's international commitment to combat forced labour and child labour by imposing reporting obligations on (i) government institutions producing, purchasing or distributing goods in Canada or elsewhere; and (ii) certain business entities producing goods in Canada or elsewhere or importing goods produced outside Canada.

The Canada-United States of America – Mexico Agreement ("Cusma") came into effect on July 1, 2020 and replaced the North American Free Trade Agreement implemented in 1994.

Article 23.6 of CUSMA provides:

> The Parties recognize the goal of eliminating all forms of forced or compulsory labor, including forced or compulsory child labor. Accordingly, each Party shall prohibit the importation of goods into its territory from other sources produced in whole or in part by forced or compulsory labor, including forced or compulsory child labor.

Canada was at risk of a complaint under CUSMA. The United States introduced legislation on forced labour in mid 2022. Canada lagged behind. In late 2022 an Uyghur activist raised concern that Canada (as a US trade partner) was doing little to stop the trade in forced-labour goods. The Canadian government was facing criticism in the press. According to a news article in December 2022, the score was U.S. 2398 v. Canada 1 – for the number of shipments in 2022 stopped at customs over suspicions that they contained forced-labour goods. The sole intercepted shipment, clothing from China, was let in after an appeal by the importer [The Xinjiang region is estimated to account for 20% of the world's cotton production and 80% of China's domestic cotton production]

The International Labour Organization published a report in September 2022. It reported that 27.6 million people are trapped in forced labour—an increase of 2.7 million individuals since 2016. The worsening situation is attributed to the compounding effects of the pandemic, political instability and unsafe migration in recent years.

### *Canadian Decisions on the Forced Labour Issues in 2022*

*In Kilgour v. Canada* 2022 FC 472, the applicants and an Intervener asked the Federal Court of Canada to find that the Canada Border Services Agency ("CBSA") had the authority under the *Customs Tariff*, SC 1997 c. 36 to implement a presumptive determination with respect to all goods imported from the Xinjiang region of China. They claimed all such goods had an increased likelihood of being produced using forced labour, and thus should be presumptively prohibited from import into Canada, unless the importers provided clear and convincing evidence to the contrary. The original request was made to CBSA to implement the presumptive determination. The CBSA responded that it did not have the authority to implement the presumption. The Court dismissed the application for judicial review. It noted that Held: The application for judicial review was dismissed. The Court noted that (a) CBSA reply was not a matter amenable to judicial review, (b) the applicants did not have standing to bring the application, (c) the CBSA's interpretation of the legislation was reasonable, (d) the border agency's focus on producers or importers, rather than regions or countries, and the prohibition on such goods

was correct and was correct in the application on a case-by-case basis and (e) each shipment of goods that arrives in Canada is subject to an officer's determination on origin, tariff and value, and such decisions can be appealed through administrative mechanisms.

*In Uyghur Rights Advocacy Project v. Canada*, 2023 FC 126, the Uyghur Rights Advocacy Project ("URAP") brought an application for judicial review of the acts and omissions of the Government of Canada. URAP contended that Canada, by its acts and omissions, was not respecting its international obligations under Article I of the *Convention on the Prevention and Punishment of the Crime of Genocide*, by failing to prevent – or take any steps to prevent – the ongoing genocide against the Uyghur population. This lack of action, according to URAP, contributed to the crimes committed against the Uyghur people of China. URAP asked for five declarations from the Court, namely:

1. The crime of genocide is currently being committed against the Uyghur population on the territory of the PRC, since at least 2014;
2. Canada is bound by the provisions of the *Convention*;
3. Canada knows, or should have known, that the crime of genocide is being committed against the Uyghur population since at least 2014, or alternatively;
4. Canada knows, or should have known, of the existence of a serious risk that genocide would be committed against the Uyghur population on PRC's territory; and;
5. Canada, by its acts and omissions, is in breach of article I of the *Convention*.

The Federal Court of Canada dismissed the application for judicial review noting:

> [80] As Elie Wiesel said in his Nobel Peace Prize acceptance speech on December 10, 1986: "Silence encourages the tormentor, never the tormented. Sometimes we must interfere." And as Roméo Dallaire wrote in *Shake Hands with the Devil: The Failure of Humanity in Rwanda*, his book chronicling his time spent as Force Commander of the United Nations Assistance Mission for Rwanda in 1993-94:
>
> The international community, of which the UN is only a symbol, failed to move beyond self-interest for the sake of Rwanda. While most nations agreed that something should be done they all had an excuse why they should not be the ones to do it. As a result, the UN was denied the political will and material means to prevent the tragedy.
>
> [81] The Canadian government has obligations under international law, including with respect to international treaties such as the *Convention*. A firm stance against genocide is an undeniable imperative for the world, as articulated by Elie Wiesel and Roméo Dallaire, who were witnesses to genocide. Yet, the mere potential existence of a genocide does not automatically ground proceedings before the Court.
>
> [82] Notwithstanding the gravity of the issues raised by URAP in this Application, I find that these issues are not cognizable in administrative law, nor justiciable under the political question doctrine. As this Court must

respect the dividing lines between the three branches of Government, the matters raised in this Application should be left to the executive and legislative branches until such time as those bodies enact law or policy, or make otherwise reviewable decisions.

### *Legislation in Place Prior to Bill S-211*

Canada does have legislation in place that prohibits forced labour or exploitation of labour. The legislation is not as far reaching as Bill S-211 into the supply chain.

### *The Criminal Code of Canada provides:*

> *Criminal Code of Canada* - 279.04
> Exploitation
> 1. For the purposes of sections 279.01 to 279.03, a person exploits another person if they cause them to provide, or offer to provide, labour or a service by engaging in conduct that, in all the circumstances, could reasonably be expected to cause the other person to believe that their safety or the safety of a person known to them would be threatened if they failed to provide, or offer to provide, the labour or service.
>
> Factors
> 2. In determining whether an accused exploits another person under subsection (1), the Court may consider, among other factors, whether the accused
> (a) used or threatened to use force or another form of coercion;
> (b) used deception; or
> (c) abused a position of trust, power or authority.

The *Canada Labour Code* (which applies to employees of federal undertakings) provides:

> 178 Minimum wage
> 1. Except as otherwise provided by or under this Division, an employer shall pay to each employee a wage at a rate
>
> 2. (a) not less than the minimum hourly rate fixed, from time to time, by or under an Act of the legislature of the province where the employee is usually employed and that is generally applicable regardless of occupation, status or work experience; or
> (b) where the wages of the employee are paid on any basis of time other than hourly, not less than the equivalent of the rate under paragraph (a) for the time worked by the employee.

The *Crimes Against Humanity and War Crimes Act (2000)* is a relatively new piece of legislation. Section 6 provides:

> Genocide, etc., committed outside Canada
> 1. (1) Every person who, either before or after the coming into force of this section, commits outside Canada
> (a) genocide,
> (b) a crime against humanity, or
> (c) a war crime, is guilty of an indictable offence and may be prosecuted for that offence

The legislation defines “crimes against humanity” as “murder, extermination, enslavement, deportation, imprisonment, torture, sexual violence, persecution or any other inhumane act or omission that is committed against any civilian population or any identifiable

group and that, at the time and in the place of its commission, constitutes a crime against humanity according to customary international law or conventional international law or by virtue of its being criminal according to the general principles of law recognized by the community of nations, whether or not it constitutes a contravention of the law in force at the time and in the place of its commission."

### *Bill S-211 – What Does it Seek to Accomplish and What Does it Require*

Bill S-211 has been criticized as inadequate and a "half measure". It simply requires Canadian institutions and private sector businesses to report the steps they have taken to prevent and reduce the risk of forced labour and child labour used at any step of the production of goods.

Companies caught by the Bill are required to file a report by May 31st of each year.

The idea is that over time, this increased compliance attention will discourage upstream suppliers from engaging in such practices if they want to continue supplying goods to the Canadian market.
Reporting entities include all Canadian federal government institutions and departments, Crown corporations and their wholly-owned subsidiaries, as well as any other private sector "entity"

It applies to any "entity" that is:

1. producing, selling or distributing goods in Canada or elsewhere;
2. importing into Canada goods produced outside Canada; or
3. controlling an entity engaged in any activity described in paragraph (1) or (2), with control defined broadly as any direct or indirect control or common control "in any manner".

"Entity" is defined as: as a corporation or a trust, partnership or unincorporated organization that is:

1. is **listed on a stock exchange** in Canada;
2. has a **place of business in Canada, does business in Canada or has assets in Canada** and that, based on its consolidated financial statements, **meets at least two of the following conditions** for at least one of its two most recent financial years:
    1. it has at least C$20 million in assets,
    2. it has generated at least C$40 million in revenue, and
    3. it employs an average of at least 250 employees;

or

1. is otherwise prescribed by regulations, (which have yet to be enacted)

Reports must include:

1. the entity's structure, activities and supply chains;
2. its policies and its due diligence processes in relation to forced labour and child labour;
3. the parts of its business and supply chains that carry a risk of forced labour or child labour being used and the steps it has taken to assess and manage that risk;
4. any measures taken to remediate any forced labour or child labour;
5. any measures taken to remediate the loss of income to the most vulnerable families that results

from any measure taken to eliminate the use of forced labour or child labour in its activities and supply chains;

6. the training provided to employees on forced labour and child labour; and

7. how the entity assesses its effectiveness in ensuring that forced labour and child labour are not being used in its business and supply chains.

Bill S-211 contains additional elements of note:

1. It extends the import ban under Canada's *Customs Tariff* to goods that are «mined, manufactured or produced wholly or in part» with «child labour» in addition to goods produced with «forced labour» and «prison labour» which are already prohibited.

2. It codifies a Canadian definition of both "child labour" and "forced labour", adopting the definitions from Article 3 of the International Labour Organization (ILO) Worst Forms of Child Labour Convention, 1999 and Article 2 of the ILO Forced Labour Convention, 1930 respectively.

3. It introduces a definition of "production of goods" meaning "the manufacturing, growing, extracting and processing of goods."

4. It gives new enforcement powers to the Minister of Public Safety and Emergency Preparedness, including powers of search, inspection and seizure of documents and evidence.

5. **Importantly, Bill S-211 also creates personal liability for directors and officers, among others, who direct, authorize, assent to, acquiesce in or participate in an offence under the proposed act.**

The Bill does not prescribe the specific measures that a company must take to remediate forced labour or child labour in its supply chains. It also doesn't state the steps they have to take to prevent and reduce the risk of forced labour and child labour used at any step of the production of goods. There is no guidance on what inquiries a company has to make downstream the supply chain. Is a survey of their suppliers sufficient? Should they require declarations from suppliers? Should they incorporate warranties in supply contracts, together with reporting requirements? How should a company structure its procurement process? How is this achieved if multiple intermediaries are involved?

At a minimum an entity must take certain steps. These should include:

1. Conducting due diligence to both identify any forced labour or child labour in their respective supply chains and track the effectiveness of certain frameworks and policies to ensure that the risk of forced labour and child labour is reduced. See for example the United Nations Business and Human Rights Navigator – Due Diligence Considerations[1];

1 https://bhr-navigator.unglobalcompact.org/issues/forced-labour/due-diligence-considerations/

2. Implementing supplier codes of conduct setting out certain necessary prohibitions and monitoring procedures regarding suppliers' labour practices and, specifically, the use of forced labour or child labour;
3. Training directors, officers and internal personnel on their duties in light of the obligations under Bill S-211; and
4. Proactively reviewing and updating contracts with existing suppliers to ensure that any risks associated with forced labour or child labour are promptly addressed and mitigated.

The reports required under Bill S-211 must be approved by each respective entity's governing body and such approval must be "evidenced by the signature of one or more members of the governing body of each entity that approved the report." This leads to the question as to whether the individuals signing the reports can also be held personally liable for any misrepresentations in the report. The government has indicated its intention to hold directors and officers accountable for the disclosure required under the legislation and, based on the current wording, if any such persons direct, authorize, assent to acquiesce in or participate in knowingly providing false or misleading information, they can be fined up to $250,000. The Bill grants the Minister extensive search powers of premises including residential properties.

Obviously supply chain transparency should be a vital part of any company's ESG framework. The rise of ESG reporting requirements has put pressure on companies to "greenwash." This has resulted in a sharpened focus of regulators and activist investors through legal proceedings. The cost of inaction may be the greatest impact of Bill S-211.

## Mitigating Cyber Risk in the Trucking Sector

By Jamal Rehman

As the transportation, logistics, and supply chain sectors increasingly shift towards the adoption of artificial intelligence, automation, and the implementation of digital infrastructures - which include connected technologies and cloud-based storage solutions – so too does the risk of cybersecurity attacks and breaches of privacy.

The transportation sector in particular carries a unique scope of what is termed "cyber risk" given the complex latticework of supply chain and logistics in which it operates. Ordinarily, this includes the multitude of actors, such as shippers, brokers, intermediaries, steamship lines, rail, and other carriers, to which they face pressures from and obligations to.

The risk is particularly enhanced for small businesses, who often lack the resources, training, and personnel when compared to their larger counterparts.

The cybersecurity of any business requires serious consideration, given the increasingly complex lines of attack used by modern attackers, as well as the potentially catastrophic consequences of an attack, which can include large extorted payouts, fatal reputational damage, and loss of customer and brand confidence, all of which affect without question can affect the bottom line.

An introduction, this article will focus on the two most common cyber attacks faced by business

across the trucking sector, which can be categorized into the two following categories: (i) ransomware; and (ii) phishing.

## Ransomware

As the name suggests, ransomware is an extortionary software designed to lock a user or organization access to their computers, servers, or devices. Ransomware locks these devices and demands a ransom payment in exchange for returned access.

Many affected businesses wrongfully believe that simply paying the ransom represents the path of least resistance when it comes to regaining access to their devices. This misconception lies at the root of the attack and only serves to improve its effectiveness.

In practice, a ransomware attack usually looks like an employee opening a seemingly harmless email or link contained within an email, with the user then being "locked out" followed by a message demanding payment in exchange for resumed access. These incidents are known as "single-extortion" attacks.

However, as is usually the case with crime, ransomware attacks have become increasingly complex, with some attackers implementing "double-extortion" (i.e. adding the threat of stealing a victim's data and posting it online) or even "triple-extortion" (i.e. adds the additional threat of using the stolen data to attack or harass a business's customers of business partners, which in this case, can include any number of entities along the supply chain)

## Phishing

By contrast, phishing is a type of attack specifically geared towards the theft of sensitive personal or financial information.

Phishing messages usually take the form of an email, phone call, text message, or other form of message on a social media platform from an attacker who is posing as a reputable person (i.e. President or CEO of the business) or entity (i.e. bank, law firm, etc.), and tries to trick the user into clicking a malicious link or download malicious software (or malware, as it's more commonly known), so as to entice the user to share sensitive information, such as a social security number, bank account number, or credit information.

Phishers often use public sources of information, such as LinkedIn Facebook, Twitter, and company directories to gather their target's personal details, work history, interests, and activities, which taken together are used to craft a highly targeted, believable message.

## Preventing Cyber Attacks

Here are four simple steps a business can take to protect itself from cybersecurity breaches:

1. **Consider hiring an accredited IT security professional**

Hiring an IT security professional, preferably one with industry-recognized certifications (such as an Certified Information Security Manager, or "CISM"), who can assess risks, implement effective governance, and proactively respond to incidents, is a great first step to strengthening the digital front line.

2. **Provide proper education and training to employees**

Given that employees are the biggest risk factor, it is critical that they be provided with routine training with respect to identifying and reporting suspicious online activity.

With the workforce becoming increasingly remote, proper training becomes all the more important.

The culture and resources of a business are unique and so too should the training regimen be when it comes to cyber safety and risk prevention. However, it is generally recommended that

routine training regimens include: the common techniques used by attackers, the typical characteristics of harmful or suspicious messages, the consequences of a breach, and how to properly report a suspicious incident when faced with one in real time. "Test breaches", as they are termed, are a particularly effective learning tool.

3. **Know obligations should a breach occur**

There is no strategy that is 100% effective in preventing a cyber breach. A business can do everything right and still fall victim to an attack.

As such, a business should have an emergency response plan in place, which includes an emergency contact list including insurers, legal counsel, and law enforcement authorities at the top of that list.

The *Personal Information Protection and Electronic Documents Act*, which applies trucking corporations and indeed to all private sector organizations across Canada, also makes it mandatory for organizations to do the following: report to the Privacy Commissioner of Canada any security breaches involving personal information which poses a real risk of significant harm to individuals; notify the affected individual(s) about those breaches; and to maintain records of all said breaches.

4. **Get cybersecurity insurance**

Cybersecurity insurance is designed to support and protect businesses from cyber risk.

Specifically, cybersecurity insurance can offer protection against financial losses caused by incidents such as phishing, online extortion, and identity theft.

Some insurers offer cyber insurance as an "add on" to an existing policy, but businesses are also generally able to purchase this coverage separately.

In many instances, cybersecurity insurance also offers the added benefit of providing coverage for network repair, legal claims, and even public relations services in some cases, to help rebuild trust from the customer base.

Cybersecurity insurance in today's digital marketplace is a must, no longer just a "nice to have".

## Mitigating Cyber Risk in the Trucking Sector

By Saisha Mahil

Federally regulated trucking companies should be aware of changes to the termination provisions under Part III of the *Canada Labour Code* ("**Code**") that are coming into effect as of February 1, 2024.

The Code applies to all road transportation services, including trucks and buses, that cross provincial or international borders. In other words, if you operate, or are employed by, a trucking company that performs services interprovincially and/or to the United States of America, that company would be subject to the Code.

Previously, employees with three consecutive months or more of continuous employment were entitled to two weeks' notice or pay in lieu of notice upon being terminated without cause. Once the new provisions come into effect on February 1, 2024, such notice period increases to three weeks. The notice period continues to increase by one week for each additional year of service completed thereafter, up to a maximum of eight weeks. Employers who provide notice before February 1, 2024 will not be required to follow the new provisions.

The new provisions also require federally

regulated trucking companies to provide a written statement of benefits to employees who are terminated. The statement must set out the employee's vacation benefits, wages, severance pay and any other benefits and pay arising from their employment with the employer as of the date of the statement. The statement must be given to the employee as follows:

1. If the employee is given advance working notice of termination, no later than two weeks before the date of the termination; or
2. If the employee is given pay in lieu of notice, no later than the date of the termination.

## General Considerations for Federally Regulated Trucking Companies

In order for a person to gain the protection afforded to employees under Part III of the Code, a worker must have status as an employee. It is therefore important that federally regulated trucking companies that engage both employee drivers and owner-operators (i.e., independent contractors) ensure that they have in place well-drafted owner-operator and/or employment agreements. In addition to written agreements, trucking companies (especially those that engage owner-operators) must ensure that they examine the totality of their relationships with their own owner-operators to determine if a person is truly an owner-operator or if they may inadvertently be classified as an employee.

## Considerations for Federally Regulated Trucking Companies that Hire Employees

Federally regulated trucking companies should consider auditing their employment agreements to ensure that the agreements provide at least the minimum notice of termination provided under the Code. This is especially important in light of recent case law (*Waksdale v. Swegon North America Inc.*, 2020 ONCA 391) which effectively heightens the risk that contracting out of the minimum standards required by the Code may render the termination clauses in an offending employment contract unenforceable. If a termination clause in an employment agreement is rendered unenforceable, this could increase the amount of pay in lieu of notice payable to an employee upon termination without cause.

## Considerations for Federally Regulated Trucking Companies that Engage Owner-Operators

Federally regulated trucking companies that engage owner-operators should have in place a carefully drafted owner-operator agreement that clearly identifies the owner-operator as being an independent contractor. Apart from having a written contract, federally regulated trucking companies should ensure that their interactions with an intended owner-operator is not at risk of being characterized as an employer-employee relationship. If an owner-operator is classified as an employee, that owner-operator would then be entitled to notice or pay in lieu of notice under the Code. Trucking companies should therefore ensure that owner-operators own their own trucks, have the ability to control when they work, are responsible for their own fuel and insurance expenses, and pay for their own truck maintenance, among other things.

## Contact us

If you have a Transportation & Logistics Group matter and are in need of legal advice, please do not hesitate to contact Rui M. Fernandes, at 416.203.9505 or rfernandes@grllp.com.

*(This newsletter is provided for educational purposes only, and does not necessarily reflect the views of Gardiner Roberts LLP.)*