Aon Risk Solutions
Financial Services Group

At-a-Glance

Issue 69 May 2018

In this Issue

Goodlife Fitness settles massive wage-and-hour class action

Goodlife Fitness, one of the most recognizable fitness chains in the Canadian industry, recently settled a class-action lawsuit for $7.5 million over unpaid wages. Brought on behalf of all current and former non-managerial employees who worked for Goodlife in its Ontario locations since October 2014, the lawsuit alleged that the company failed to accurately compensate employees for hours worked, including overtime. The lawsuit was initially filed in October 2016 seeking $60 million in unpaid wages; it was later expanded to include employees nationwide in January 2017.

The lawsuit contained allegations that Goodlife violated employment standards legislation and its contracts of employment by requiring employees to work hours above those scheduled, including hours both above and below the overtime threshold, while failing to appropriately compensate them as required. Interestingly, in 2016 certain Goodlife employees elected to unionize and became represented by the Workers United Canada Council. These employees were excluded from the class-action lawsuit as of the time they became unionized.

Personal trainer employees will obtain approximately $5.5 million from the settlement, with fitness advisors receiving around $800,000. Employees with other job classifications will be compensated from the remainder of the settlement proceeds. Employment practices liability (EPL) insurance provides coverage to employers for employment-related claims made by employees alleging issues such as discrimination, wrongful termination or harassment. In some cases, an endorsement for an EPL insurance policy can be procured to provide sublimited defence costs coverage for an organization embroiled in a wage and hour lawsuit. In other cases, it may be achievable for clients to purchase standalone coverage for settlements and judgments resulting from lawsuits seeking unpaid wages through select Bermuda carriers. However, the price and retention for such insurance is relatively high. An experienced insurance broker can assist you in evaluating your company's risk exposure and recommending an appropriate risk transfer solution.

Securities class action lawsuits in the U.S. just got more complicated

In a seminal decision of the U.S. Supreme Court, released on 20 March 2018, a unanimous bench ruled that plaintiffs are permitted to bring class action securities lawsuits under the *Securities Act of 1933* (1933 act) in state courts. Cyan, Inc. v. Beaver County Employees Retirement Fund (Cyan) has muddied the waters of a securities litigation system over 85 years in the making. Pre-Cyan, multiple securities law statutes in the U.S. had created a framework in which related securities class action lawsuits involving nationally traded securities were considered together, simultaneously, in federal court. Now, according to the Supreme Court's interpretation of the 1933 act in Cyan, state courts also have jurisdiction to adjudicate class action securities lawsuits under the 1933 act.

Criticisms of the decision point to the inefficiency and wasted resources a bifurcated system would promote by allowing two closely related lawsuits, often with the same or similar facts and allegations, to proceed in different venues, on different timelines, with two different sets of court procedures and practice rules. The defendant would likely face an enormous burden in attempting to defend two lawsuits at once. There are also certain legislative protections available to defendants when related cases are consolidated, such as an automatic stay of discovery where a motion to dismiss is pending and heightened pleading standards for plaintiffs, that will be lost. Defence counsel will need to balance a multitude of strategic considerations when defending concurrent actions.

At this point in time, it is impossible to predict the impact that Cyan will have on securities class action lawsuits in the U.S. However, experience has demonstrated that when there is a fundamental shift in the law such as this, the status quo rarely remains. As such, it is prudent for organizations with U.S. exposure to consider risk transfer solutions to assist in mitigating the adverse financial effects of defending parallel lawsuits. A directors' and officers' liability insurance policy can provide coverage for settlements, judgements and defence costs to both individual directors and officers, and the organization, in the event of a securities lawsuit.

U.S. Court of Appeal rules no coverage for social engineering fraud claim

In the 17 April 2018 decision of Aqua Star (USA) Corp. v. Travelers Casualty and Surety Company of America, the Ninth Circuit Court of Appeals ruled that no coverage was available under the computer fraud insuring agreement of the plaintiff's commercial crime policy for losses stemming from social engineering fraud. Aqua Star (USA) Corp. (Aqua Star) imported seafood and had an ongoing relationship with Longwei, a legitimate vendor. After emails between employees of Aqua Star and Longwei were monitored and ultimately intercepted, the hacker used a "spoof" email domain to instruct the Aqua Star employee to change the bank account information on record for Longwei. This new, fraudulent payment information was then communicated to Aqua Star's bank, which resulted in $713,890 being wired to a fraudulent account before the social engineering scheme was detected.

Aqua Star had a commercial crime policy in force at the time of the loss, which provided coverage for the company's "direct loss of…Money, Securities, and Other Property directly caused by Computer Fraud." In denying coverage, the insurer, Travelers, relied on an exclusion in the policy which precluded coverage for loss resulting from "the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System." In upholding the District Court's summary judgment ruling in favour of the insurer, the Ninth Circuit found that the exclusion applied and no coverage was available, as Aqua Star's losses resulted from employees who had "the authority to enter" its computer system.

In keeping with precedent decisions in the area, the court reaffirmed the dividing line between social engineering coverage and related computer fraud coverage under a commercial crime policy. To address the continued loss trend in this area, most markets have released a social engineering fraud endorsement that can be added for an additional premium to a crime policy. These endorsements are usually sublimited; however, full limits are offered by some markets, albeit typically with a call-back requirement as a precondition to coverage. Although extra premium is required for this coverage, given the increasing prevalence of social engineering fraud, organizations would be wise to consider adding it to their existing crime policy.

Items of Note

- On 23 March 2018, Congress enacted The Clarifying Lawful Overseas Use of Data (CLOUD) Act as part of the Omnibus Spending Bill signed by U.S. President Donald Trump. Amending the Stored Communications Act, the legislation compels U.S. providers of "electronic communication service or remote computing" to comply with requests from U.S. law enforcement to obtain the information of U.S. citizens from servers located outside the U.S. The foreign country must have signed an agreement to share data with the U.S., but, notably, there are no minimum privacy or human rights law standards imposed on the foreign nation as a condition to entering into such an agreement. Practically speaking, each party to the agreement will be permitted to access the data of the other country's citizens without government approval.
- The U.S. Securities and Exchange Commission has levied a $35 million penalty against Altaba, Inc. (successor in interest to Yahoo! Inc.) for Yahoo's two year delay in reporting the massive cybersecurity breach that initially occurred in December 2014. The penalty settles charges that Yahoo misled investors by failing to disclose the breach, in which hackers stole personal identifiable information pertaining to millions of user accounts. This marks the first data breach disclosure enforcement penalty in the U.S.
- As part of the Ontario government's initiative to advance women's economic empowerment and build fairer workplaces, the Ontario government recently introduced Bill 203, Pay Transparency Act, 2018. The bill creates requirements for employers regarding the disclosure of compensation information to current and prospective employees, and also imposes formal reporting obligations detailing any existing compensation gaps based on gender and other specified diversity characteristics. The bill passed Third Reading on 26 April 2018, making Ontario the first province to pass legislation of this type. The act is expected to come into force on 1 January 2019.
- On 25 May 2018 the European Union's (EU's) General Data Protection Regulation (GDPR) will come into force. Intended to harmonize privacy laws across Europe, the regulation will apply to Canadian companies that process personal information of EU residents. Fines and penalties for non-compliance can reach exorbitant amounts – up to the greater of €10 million or 2% of an organization's global annual turnover for contraventions related to technical measures, such as breach notifications or impact assessments; or €20 million or 4% of an organization's global annual turnover for non-compliance with key provisions of the GDPR, such as transfers of personal data outside the EU to countries or organizations that do not ensure an "adequate level of protection."

Key Contacts

Brian Rosenbaum LL.B
Senior Vice President and National Director
Financial Services Group
Legal and Research Practice
t +1.416.868.2411
brian.rosenbaum@aon.ca

Desiree Money, CAIB, CRM
Senior Vice President and Regional Manager
Financial Services Group
t +1.403.267.7754
desiree.money@aon.ca

Denise Hall
Senior Vice President and National Broking Leader
Financial Services Group
t +1.416.868.5815
m +1.416.953.3280
denise.hall@aon.ca

Catherine Richmond, LL.B., CRM
Senior Vice President and Regional Manager
Financial Services Group
t +1.604.443.2429
m +1.604.318.5470
catherine.richmond@aon.ca

Catherine Lanctôt B.A.
Vice President and Manager
Financial Services Group
t +1.514.840.7008
catherine.lanctot@aon.ca

Alexis Rivait
Vice President and Team Leader
Financial Services Group
t +1.416.868.5597
alexis.rivait@aon.ca