At-a-Glance

Issue 76 March 2019

In this Issue

U.S. derivative lawsuit stemming from data breach settles for $29M

Although we haven't yet witnessed the trend in Canada, there have been several shareholder derivative lawsuits filed against boards south of the border in connection with large scale data breaches. However, none of these cases ultimately saw the plaintiffs obtain a significant monetary recovery – the majority fell at defendants' motions to dismiss, while others settled for solely the amount of plaintiffs' attorneys' fees. A recent milestone case has experienced a different outcome though, with plaintiff's obtaining a substantial settlement.

In September 2016, Yahoo! Inc. (Yahoo) publicly revealed a data breach that had taken place two years prior, affecting the personal identifiable information (PII) of up to 500 million users. Later that year, in December 2016, the company announced a second breach that had occurred three years prior in 2013, compromising PII of potentially all of Yahoo's 3 billion users. A multitude of lawsuits ensued, both in Canada and the U.S. Shareholders in the U.S. filed both a securities class action lawsuit and a derivative lawsuit, which were ultimately consolidated and collectively alleged breach of fiduciary duty, unjust enrichment, insider trading, and waste against various defendants including Yahoo, Yahoo's board of directors and certain officers and senior managers. The plaintiffs claimed that Yahoo executives and board members were aware of the privacy breaches prior to public disclosure and, moreover, that the individual defendants sought to cover up the breaches. The complaint also noted that many individual defendants sold their personal shares after the data breaches had taken place but before the public was informed of such. Verizon, which ultimately acquired the assets of Yahoo, was also named in the litigation for allegations of aiding and abetting. Verizon had initially announced plans to acquire Yahoo in July 2016. Following Yahoo's disclosure of the data breaches, Verizon negotiated a $350 million reduction in the acquisition price.

Recently, in January 2019, the Superior Court of the State of California approved a settlement of $29 million pertaining to the lawsuit. It has been stated that the amount will be funded by insurers of both the individual defendants and Verizon, as agreed to and allocated between the two parties. Only time will tell whether this recent settlement will evidence a change in tide in data breach related derivative litigation recovery or be remembered as an outlier for its substantial settlement. A directors' and officers' (D&O) liability insurance policy can provide coverage for individual board members and executives when faced with management liability claims, including those brought derivatively by shareholders. A D&O policy could also provide the corporate entity with coverage if named in a securities lawsuit. Although entity coverage for securities claims has typically been restricted to lawsuits involving the named insured's own securities, it may now be possible, in very limited circumstances, for some insureds to obtain a form of 'aiding and abetting' coverage, which would extend coverage to claims filed by shareholders of a target company in the context of an acquisition.

AON
Empower Results®

OSFI releases new reporting guidelines for technological and cyber security incidents

The Office of the Superintendent of Financial Institutions (OSFI), regulator of federally registered banks and insurers, trust and loan companies, and private pension plans subject to federal oversight, issued an Advisory on Technology and Cyber Security Incident Reporting on 24 January 2019. The new guidelines, effective 31 March 2019, will apply to all federally regulated financial institutions (FRFIs) and supersede any prior guidance on cyber security incident reporting released by OSFI.

Under the new guidance, technology or cyber security incidents of a "high or critical severity level" should be reported to OSFI "as promptly as possible, but no later than 72 hours". The FRFI has discretion to determine incident materiality, with OSFI noting that "FRFIs should define incident materiality in their incident management framework". However, OSFI does provide a list of criteria that may apply to a "reportable incident", which includes the following:

- Significant operational impact to critical information systems or data;
- Material impact to FRFI operational or customer data, including confidentiality, integrity or availability of such data;
- Significant levels of system/service disruptions;
- Extended disruptions to critical business systems/operations;
- Number of external customers impacted is significant or growing;
- Negative reputational impact is imminent (e.g. public/media disclosure);
- Material impact to critical deadlines/obligations in financial market settlement or payment systems;
- Significant impact to a third party deemed material to the FRFI;
- Material consequences to other FRFIs or the Canadian financial system; and
- The incident has been reported to the Office of the Privacy Commissioner or local/foreign regulatory authorities.

The initial incident notification to OSFI should include details regarding the date/time at which the incident was assessed to be material, as well as information regarding when the incident initially took place, the severity and type (i.e. malware, data breach, extortion) of the incident, the current status of the incident as well as planned mitigation actions, and the date of internal incident escalation to senior management and/or board members. Reporting obligations are ongoing, with OSFI expecting the FRFI to provide regular updates as new information becomes available. Following the incident, FRFIs are obligated to provide OSFI with a post-incident review report, which includes lessons learned.

Cyber liability insurance contains valuable first party coverage that can help businesses mitigate the financial effects of both technology and cyber risk. If a company experiences a data breach or covered cyber security incident, cyber insurance could respond to provide coverage for expenses associated with reporting to and communicating with regulatory, supervisory or administrative authorities, such as OSFI. A cyber policy may also respond to provide first party breach response services and indemnity for related notification and credit/identity theft monitoring costs. Third-party liability coverage may also be available for settlement and judgment amounts, as well as legal fees, in the event that the organization later faces a civil lawsuit or regulatory investigation or proceeding stemming from a cyber security incident.

Key Contacts

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

David Quail, M.Sc., CRM
Vice President and Regional Manager
Financial Services Group
t +1.403.267.7066
david.quail@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

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