



Coup d'œil

Dans ce numéro :

- 1 Aux États-Unis, une action dérivée découlant d'une atteinte à la protection des données est réglée à l'amiable pour 29 M\$
- 2 Le BSIF publie de nouvelles lignes directrices eu égard au signalement des incidents liés à la technologie et à la cybersécurité
- 3 Personnes-ressources clés

Aux États-Unis, une action dérivée découlant d'une atteinte à la protection des données est réglée à l'amiable pour 29 M\$

Même si cette tendance n'a pas encore cours au Canada, plusieurs actions dérivées ont été intentées par les actionnaires contre les conseils d'administration au sud de la frontière, à la suite de piratages de données à grande échelle. Toutefois, les demandeurs n'ont finalement pas obtenu de sanction pécuniaire majeure dans aucun de ces cas. La plupart des cas ont été déboutés, tandis que d'autres ont été réglés à l'amiable pour le seul montant des honoraires des avocats des demandeurs. Une affaire récente a pourtant abouti à une autre conclusion, quand le demandeur a obtenu un règlement substantiel.

En septembre 2016, Yahoo! Inc. (Yahoo) a publiquement révélé une atteinte à la protection des données survenue deux ans plus tôt, qui concernait les données personnelles identifiables de près de 500 millions d'utilisateurs. En décembre de la même année, la société a révélé une deuxième atteinte à la protection des données, survenue trois ans plus tôt, en 2013, qui avait compromis les données personnelles identifiables de la plupart des 3 milliards d'utilisateurs de Yahoo. De nombreuses actions ont alors été intentées, au Canada et aux États-Unis. Aux États-Unis, les actionnaires ont intenté un recours collectif en valeurs mobilières ainsi qu'une action dérivée. Les deux actions ont finalement été regroupées dans une même poursuite pour manquement présumé à l'obligation fiduciaire, enrichissement injustifié, délit d'initiés et gaspillage contre divers défendeurs, notamment Yahoo, le conseil d'administration de Yahoo et certains administrateurs et membres de la haute direction. Les demandeurs ont allégué que les dirigeants et les membres du conseil d'administration de Yahoo étaient au courant de l'atteinte à la vie privée avant la divulgation publique et, qui plus est, que les défendeurs individuels avaient cherché à couvrir les infractions. Dans la plainte, il était également stipulé que plusieurs défendeurs individuels avaient vendu leurs actions personnelles après la violation des données, mais avant que le public n'en ait été informé. Verizon, qui a finalement acquis les actifs de Yahoo, était également citée dans la poursuite dans le cadre d'allégations de complicité. À l'origine, Verizon avait prévu d'acquérir Yahoo en juillet 2016. À la suite de la divulgation du piratage des données de Yahoo, Verizon a négocié une réduction de 350 millions de dollars sur le prix d'acquisition.

Récemment, en janvier 2019, la Cour supérieure de l'État de Californie a approuvé un règlement à l'amiable de 29 millions de dollars relativement à la poursuite. Il a été stipulé que cette somme serait financée par les assureurs des défendeurs individuels et de Verizon, comme convenu et réparti entre les deux parties. Seul l'avenir nous dira si ce récent règlement attestera d'un revirement de la tendance en matière de recouvrement des actions dérivées liées à une violation des données ou s'il fera figure d'exception en tant que règlement substantiel. Une assurance responsabilité civile des administrateurs et des dirigeants peut offrir une protection aux membres du conseil d'administration et aux cadres supérieurs individuels lorsque ces

derniers font face à des réclamations fondées sur la responsabilité de la direction, y compris les réclamations intentées par les actionnaires. Une assurance des administrateurs et des dirigeants peut également couvrir une personne morale citée dans un procès portant sur des valeurs mobilières. La couverture des entités pour les poursuites liées à des valeurs mobilières se limitait habituellement aux poursuites portant sur les valeurs mobilières appartenant en nom propre aux assurés désignés. Toutefois, certains assurés peuvent désormais, dans certains cas très précis, obtenir une forme de couverture pour « complicité », qui étend la couverture aux poursuites intentées par les actionnaires d'une société cible dans le contexte d'une acquisition.

Le BSIF publie de nouvelles lignes directrices eu égard au signalement des incidents liés à la technologie et à la cybersécurité

Le Bureau du surintendant des institutions financières (BSIF), organisme de réglementation des banques et assureurs immatriculés au fédéral, des sociétés de fiducie et de prêt et des régimes de retraite privés assujettis à la réglementation fédérale, a publié le 24 janvier 2019 le document Signalement des incidents liés à la technologie et à la cybersécurité. Les nouvelles lignes directrices, qui entreront en vigueur le 31 mars 2019, s'appliqueront à l'ensemble des institutions financières fédérales (IFF) et remplaceront toute autre consigne antérieure du BSIF relativement au signalement d'incidents liés à la cybersécurité.

En vertu de la nouvelle consigne, les incidents liés à la technologie et à la cybersécurité d'un « niveau de gravité élevé ou critique » doivent être signalés au BSIF « le plus rapidement possible, et au plus tard 72 heures après ». Il revient à l'IFF de déterminer l'importance de l'incident : le BSIF stipule que « les IFF doivent définir l'importance relative des incidents dans leur cadre de gestion des incidents ». Toutefois, le BSIF fournit une liste de critères susceptibles de s'appliquer à un « incident à signaler », notamment :

- Répercussions opérationnelles importantes sur les systèmes d'information ou les données critiques;
- Répercussions importantes sur les données opérationnelles ou sur les données des clients de l'IFF, y compris sur les plans de la confidentialité, de l'intégrité ou de la disponibilité de ces données;

- Niveaux importants de perturbation des systèmes et des services;
- Perturbations prolongées des systèmes et activités essentiels;
- Nombre important ou croissant de clients externes touchés;
- Répercussions négatives imminentes sur la réputation (p. ex., divulgation publique/médiatique);
- Répercussions importantes sur les échéances/obligations cruciales rattachées aux systèmes de règlement ou de paiement des marchés financiers;
- Répercussions importantes sur un tiers essentiel pour l'IFF;
- Conséquences importantes pour les autres IFF ou pour le système financier canadien;
- Un incident concernant une IFF a été signalé au Commissariat à la protection de la vie privée du Canada ou aux organismes de réglementation canadiens/étrangers.

Le signalement initial de l'incident au BSIF doit inclure des détails quant aux date et heure où l'incident a été classifié important, ainsi que des renseignements quant aux date et heure/période où l'incident est survenu, le niveau de gravité de l'incident et le type d'incident (p. ex., malicieux, violation de données, extorsion), l'état actuel de l'incident ainsi que les mesures d'atténuation prévues et la date

du signalement de l'incident à la haute direction ou au conseil d'administration. Les exigences de signalement sont constantes; le BSIF s'attend à ce que les IFF fassent périodiquement le point à mesure que de nouveaux renseignements deviennent disponibles. Après l'incident, l'IFF doit rendre compte au BSIF de son analyse post-incident et des leçons apprises.

L'assurance de responsabilité en matière de cyberresponsabilité contient une couverture précieuse pour l'assuré pouvant aider les entreprises à atténuer les incidences financières du risque technologique et du cyberrisque. Si une société est victime d'une atteinte à la protection des données ou d'un incident lié à la cybersécurité couvert, la cyberassurance peut intervenir pour couvrir les frais liés au signalement et à la communication aux organismes de réglementation, de supervision ou d'administration, tel le BSIF. Une cyberassurance peut également fournir des services d'intervention de premier plan en cas d'atteinte et une indemnité pour les frais de notification et de surveillance du crédit et de l'identité associés. L'assurance responsabilité civile peut également inclure les frais liés au règlement et au jugement, ainsi que les frais judiciaires, dans le cas où une poursuite civile ou une enquête ou une procédure réglementaire serait engagée ultérieurement contre l'organisation à la suite d'un incident lié à la cybersécurité.

Personnes-ressources clés

Alexis Rivait

Vice-présidente et Chargée de compte
Groupe services financiers
t +1.416.868.5597
alexis.rivait@aon.ca

David Quail, M.Sc., CRM

Vice-présidente et Chargée de compte
Groupe services financiers
t +1.403.267.7066
david.quail@aon.ca

Denise Hall

Vice-présidente principale et responsable nationale de courtage
Groupe services financiers
t +1.416.868.5815
m +1.416-953.3280
denise.hall@aon.ca

Catherine Richmond, LL.B., CRM

Vice-présidente principale et Chargée de compte
Groupe services financiers
t +1.604.443.2429
m +1.604.318.5470
catherine.richmond@aon.ca

Catherine Lanctôt B.A.

Vice-présidente et Directrice
Groupe services financiers
t + 1.514.840.7008
catherine.lanctot@aon.ca

Brian Rosenbaum LL.B

Vice-président principal et Directeur national
Pratique des affaires juridiques et des recherches
Groupe services financiers
t +1.416.868.2411
brian.rosenbaum@aon.ca

À propos d'Aon

Aon plc (NYSE : Aon) est un des principaux cabinets mondiaux de services professionnels, fournissant un vaste éventail de solutions de risques, de retraite et de santé. Nos 50 000 employés dans 120 pays donnent à nos clients les moyens de prospérer en utilisant des données exclusives et analytiques pour communiquer des informations qui réduisent la volatilité et améliorent le rendement.

© Aon Reed Stenhouse 2019. Tous droits réservés.

Cette publication contient des renseignements généraux et ne vise pas à fournir un aperçu des garanties. L'information n'est pas destinée à constituer des conseils juridiques ou professionnels. Reportez-vous au libellé de la police d'assurance pour vous familiariser avec les modalités, conditions, exclusions et limitations réelles de l'assurance. Pour obtenir des renseignements plus précis sur la façon dont nous pouvons vous aider, communiquez avec Aon Reed Stenhouse Inc.

