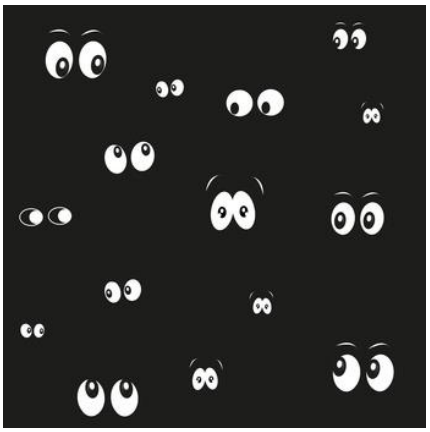
October 2016

Bulletin

Let the Right One In

No, we're not referring to the iconic Swedish vampire thriller of the same name (though we at AUM Law highly recommend it on this All Hallows' Eve). While this film will give you chills, we're willing to bet that it's the fear of letting the wrong ones into your computer systems that keeps you up at night.

There is good reason to worry, as recent revelations surrounding the not so recent Yahoo hacks have demonstrated, not to mention the high-profile security and privacy woes of Ashley Madison. We will examine these and other chilling developments (while paying homage to our favorite frightening flicks) in our annual Halloween edition of the AUM Law Bulletin.



In this bulletin

In Brief: OSC Appoints New Enforcement Director ● Common Reporting Standard to Exclude TFSAs ● Survey Says…

1. Invasion of the Data Snatchers – Yahoo and the Biggest Cyber Breach… Ever?

Whether it be in the context of the US election, Wikileaks and allegations of Russian skulduggery, or the mild inconvenience of a nation-wide Netflix outage, cybersecurity or "the cyber" as Donald Trump would say, is front and center in the news these days. The not-so coveted award for the biggest (known) hack to date, however, goes to Yahoo. The only thing more shocking than the magnitude of Yahoo's 2014 data breach, which exposed the names, email addresses, telephone numbers, dates of birth and passwords of approximately 500 million users, was the two years Yahoo took to detect the breach and notify its impacted customers.

In Brief

OSC Appoints New Enforcement Director

Earlier this month, the Ontario Securities Commission (OSC) announced the appointment of Jeff Kehoe as Enforcement Director. Mr. Kehoe joins the OSC after a decade as Director and Vice President of Enforcement at IIROC.

•

Common Reporting Standard to Exclude TFSAs

The Canadian government recently introduced legislation that will implement the Common Reporting Standard (CRS), with certain provisions excluding TFSAs and other types of accounts from the CRS.

While the regulatory impact of this breach remains to be seen, calls for a Securities and Exchange Commission (SEC) investigation into whether Yahoo failed to keep investors and the public informed, and whether the company made complete and accurate representations about the security of its IT systems, are already under way. Yahoo is also the subject of several class-action lawsuits over the intrusion.

The SEC has provided guidance on cybersecurity in the past, directing public companies to disclose risks to cybersecurity as well as disclosure of incidents that have a material impact on the company.

Canadian regulators are also taking notice of this growing threat. As mentioned in our September 2016 Bulletin, the Canadian Securities Administrators (CSA) just released its own Guidance on cybersecurity, outlining several best practices and indicating cybersecurity will be a major focus for them going forward. IIROC President and CEO Andrew Kriegler, while speaking at the recent 2016 Quebec Compliance Conference, also referenced resources IIROC had created to help firms identify and manage cybersecurity risks and threats.

As well, on October 14, 2016, the Government of Canada announced its participation in and endorsement of the G7 Fundamental Elements of Cybersecurity for the Financial Sector Guidelines (Guidelines). The Guidelines outline eight basic elements for a cybersecurity strategy and framework, consistent with guidance previously provided by other Canadian regulators including the CSA, MFDA and IIROC.

While the final regulatory and legal impact to Yahoo remains to be seen, there are certain lessons that can be drawn from the Yahoo case now. For example, cybersecurity needs to be a priority for all firms. It appears that Yahoo was slow to invest money in cyber defense and institute certain security protections. As well, this case demonstrates that it is important to be proactive and not reactive with your cybersecurity strategy and framework. Here, it appears Yahoo was slow to implement intrusion-detection tools that matched industry standards, and consequently was slow to detect the 2014 breach.

Given the heavy reputational damage, regulatory and legal risk, privacy concerns, and in Yahoo's case a possible failed sale of core operations to Verizon, the importance of a thoughtful and proactive cybersecurity strategy and framework is clear.

In the meantime, the OSC has issued a Cybersecurity and Social Media Practices Questionnaire, due on November 5th, in order to assist with the development of future staff guidance.

If you need any last minute assistance with your response to this Cybersecurity Questionnaire, or would like to discuss cybersecurity generally, please contact our Regulatory Compliance Group – we're here to help!

In Brief cont'd

As a result, Financial Institutions will not have to report TFSA account information to the CRA, or obtain self-certifications from TFSA account holders.

According to IFIC, the decision is a welcome one, as the financial services industry actively appealed for TFSAs to be excluded from the CRS.

•

Survey Says…

Several surveys have been circulated by Canadian securities regulators as of late. In addition to the Cybersecurity Questionnaire addressed more fully in this month's Bulletin, the BCSC recently released a CRM2 Survey and the OSC distributed a Compensation and Incentives Survey.

Though the deadline for the CRM2 Survey has now passed, responses to the Compensation Survey will be accepted until November 11, 2016. Please contact us if you would like assistance with the completion of this Survey.

2. The Uninvited – Ashley Madison's Unwanted Guests

Ashley Madison, a website created to facilitate extramarital affairs, could have benefited from the recent CSA guidance on cybersecurity when it suffered a cyberattack in 2015. While the breach suffered by Ashley Madison in July of 2015 was not near the scale of the massive 2014 Yahoo breach, it effectively destroyed the company's most vital asset – it's reputation for secrecy and discretion. Upon the release of personal customer information including names, addresses, and credit card information, a $578 million class action was brought by customers who incurred both reputational and financial harm.

In addition to the ongoing class action, the Office of the Privacy Commissioner (OPC) as well as the Australian Privacy Commissioner recently released their findings with respect to the data breach. In particular, the OPC found that though Avid Life Media (ALM), the private company that operates Ashley Madison, had Terms of Service that stated the security of a user's information could not be guaranteed,

as the nature of the information was highly sensitive and posed a significant risk of harm to users if disclosed, the disclaimer did not impact ALM's legal obligations under Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Not only did the OPC find that ALM should have had a higher level of security in place given the sensitive nature of the information stored, but it found that ALM did not have documented information security policies or procedures in place and only used single-factor authentication as opposed to the stronger multi-factor authentication.

The OPC also found that ALM failed to obtain informed consent from its users in two central ways. Firstly, it provided false information about its cybersecurity safeguards (including reference to a fake "Trusted Security Award"), and there was a lack of information to users about ALM's information retention practices. As such, the users' initial consent to collect personal information upon account sign up was invalid and in contravention of PIPEDA. Secondly, it found that ALM retained personal information for an indefinite period of time after account deactivation or inactivity and improperly charged users a fee (without prior notice) to withdraw their consent and have personal information erased.

The Ashley Madison case serves as an important reminder that companies should have strong Cybersecurity, Information Security and Privacy Compliance Programs in place, including appropriate policies and procedures, training and audits to ensure internal practices align with those policies and procedures. As well, it is vital to provide accurate information to customers on issues such as the security of their personal information, as their consent may be invalid in the absence of such transparency, much less deliberate misinformation. Finally, the involvement of the Australian Privacy Commissioner demonstrates the cross-border nature of privacy legislation and the need to be cognizant of, and in compliance with, the legislation of the jurisdictions you operate in.

If you are interested in discussing this decision further, receiving training on privacy legislation, or simply revisiting your current privacy policies and procedures for an update, please contact our Regulatory Compliance Group.

3. It Follows – How to Escape the Shadow of Directors' Liability

Under the *Ontario Business Corporations Act* (the OBCA) a director's resignation is only effective at the later of when the resignation is *received* by the corporation or the effective date, while under the *Canada Business Corporations Act* a director's resignation is only effective at the later of when the resignation is *sent* by the director or the effective date. In either case, it is clear that the corporation is entitled to proper notice of a resignation by a director.

In a recent decision of the Federal Court of Appeal, the court found that an *intention* to resign did not satisfy the necessary preconditions of an effective resignation under the OBCA. In this case, the corporation's lawyer was instructed to prepare the resignations of two directors, as demonstrated by the unsigned resignation documents found in the lawyer's file. The directors failed to execute and deliver the resignations, however, and as a result they were found to be personally liable as directors for the corporation's unremitted payroll tax withholdings.

This decision is a good reminder of the perils of neglecting the formalities of corporate record keeping. When tendering a resignation, it is best practice for the director to deliver his or her resignation to the corporation in writing via registered mail or courier, and insert the resignation into the corporate minute book. As well, it is wise to promptly file a Notice of Change form to ensure the public record is accurately updated.

Please contact us if you wish to discuss this or any other intricacies of corporate record keeping further.

4. When a Stranger Calls (or Emails…) – Kellogg's CASL Hassle

While the thought of receiving uninvited emails from a cereal company may not chill your blood in the same way the uninvited phone calls to Carol Kane did in 1979's cult classic *When a Stranger Calls*, it's no laughing matter for Kellogg. In response to allegations from the CRTC that Kellogg sent unsolicited commercial electronic messages (CEMs) without recipients' consent for over two months in 2014, Kellogg entered into a voluntary undertaking with the CRTC to pay a $60,000 fine and ensure that it (as well as its

third party email marketers) complied with Canada's Anti-Spam Law (CASL) going forward. By providing a voluntary undertaking to the CRTC, Kellogg avoided the risk of an administrative monetary penalty of up to $10 million per violation.

As this case demonstrates that CASL requirements can extend to third parties acting on behalf of a corporation, it is important to ensure that companies have CASL Compliance Programs in place that incorporate third party service providers. As well, as mentioned in our July 2016 Bulletin, recent CRTC Guidance confirms that in addition to obtaining the appropriate consent, it is important to maintain proper records or proof of consent once obtained. Finally, as there will be a private right of action for any person affected by a CASL contravention as of July 1, 2017, it is vital that corporations ensure their CASL Compliance Programs are up to speed.

Please contact us if you would like to discuss your CASL Compliance Program in light of recent regulatory Guidance as well as the Kellogg undertaking.

5. Angels (not Demons) - AngelList's New LaunchPad

To be clear, AUM Law is NOT endorsing the Dan Brown novel or associated film of the same name. Sorry Tom Hanks. Rather, we are referring to recent developments surrounding angel investors and the facilitation of fundraising for start-ups.

The Ontario Securities Commission (OSC) recently approved the launch of a platform in Ontario by AngelList, a U.S. based company that operates an online networking and fundraising website. The OSC decision enables accredited investors with experience in venture capital and angel investing that actively seek out AngelList to connect with other such investors and create a pool of money to be made available to a specific start-up. AngelList's role is to operate the online platform, with AngelList Advisors facilitating the syndication of offerings through the platform.

The OSC gave the green light to AngelList under its new LaunchPad initiative, a program that engages with fintech companies to provide them with guidance and flexibility in navigating securities law requirements, accelerate time-to-market, and keep securities regulation in step with digital innovation. The OSC LaunchPad was unveiled on October 24, 2016.

If you are interested in obtaining similar relief under the OSC's LaunchPad initiative, please contact our Regulatory Compliance Group.

6. Help Us Help You

As we have previously discussed, registered firms have ongoing obligations under securities legislation to inform the OSC of the following changes to a firm or a registered individual's information. Failure to notify the OSC within 10 calendar days of most of these changes may lead to a $100 late fee per day, up-to a maximum of $5,000 per year:

Changes to Firm	Changes to Registered and Permitted Individuals	Changes to Operations
• Operations (e.g., organizational structure, officers and directors) • Ownership or anticipated acquisition of securities of another entity • Insurance, auditors and constating documents (e.g., articles of amendment)	• Individual Forms 33-109F4 • Outside activities*	• Offering of new products/business lines

*The OSC has been imposing late filing fees for failure to disclose all outside activities of individuals (e.g., directors, officers, trustees, shareholders and other roles). If you are unsure what to disclose, please contact us for further analysis and potential filing.

An ounce of prevention is worth a pound of cure. Contact a member of our Regulatory Compliance Group to ensure that you are compliant.

Frequently Asked Questions

> Is there a drawback to maintaining registration in all three registrant categories – namely Exempt Market Dealer (EMD), Portfolio Manager (PM) and Investment Fund Manager (IFM)?

Many firms are registered under all three categories, whether or not they use all three. While this is a convenient approach, there are certain circumstances where this may create unintended consequences.

For example, an IFM is permitted to distribute its own product to subscribers without having an EMD registration by relying on Section 8.6 of 31-103. The exemption under Section 8.6 permits a registered advisor to sell to a subscriber without EMD registration (though as mentioned, Registrants often maintain EMD registration regardless). However, "blocker rules" prevent use of the exemption under Section 8.6. if the Registrant possesses a license that could be used to make that distribution (namely the EMD registration). This means that the registrant could be prevented from making a distribution to a subscriber under the Section 8.6 exemption if it has the EMD registration. In that case, the regulators would expect the registrant to make the distribution under its EMD license even if this would be impractical.

Fortunately, there are several approaches to dealing (pun intended) with this issue, ranging from seeking a surrender of the EMD license, to seeking comfort from the OSC that the exemption will nonetheless be relied upon in light of the blocker rules creating unintended consequences. These are but two possible avenues to take – talk to our Regulatory Compliance Group to explore these and other options further.

News & Events

Recent Speaking Engagements

Jennifer Cantwell joined NBCN's Lesley Connors at their annual conference to present 'The ever-changing landscape of AML', discussing topics such as client identification changes and expectations, and what FINTRAC looks for during reviews.

Susan Han presented at this year's Canadian Money Services Business Association's (CMSBA) Fall Conference, focusing on information emerging out of the recently released Mutual Evaluation Report from the Financial Action Task Force (FATF).

For the second year in a row, **Kimberly Poster** and **Erez Blumberger** presented the "Registration and Investment Funds" section of Osgoode Professional Development's *Intensive Course in Canadian Securities Law and Practice*, designed to teach the fundamentals of Canadian securities law in four evenings.

Erez Blumberger once again joined the TDSI Hedge Fund COO Summit as a moderator, leading two back-to-back sessions titled "Shelter from the regulatory storm: hot topics in Canadian securities regulation".