# Ashley Madison Security Breach: Lessons Learned And Valuable Recommendations For All Business

August 26, 2016

## August 26, 2016

On August 22, 2016, the Office of the Privacy Commissioner of Canada (the "OPC") released an important report regarding the Ashley Madison data breach, which exposed the personal information of some 32 million users of the online dating website marketed to people who are married or in committed relationships. As part of its investigation, held jointly with the Australian Information Commissioner, the OPC raised a number of issues regarding the security practices of Ashley Madison's parent company, Avid Life Media ("ALM"). In its report, the OPC examined the circumstances of the data breach and considered ALM's information handling practices that may have affected the likelihood or the impact of the data breach. In a section entitled "Takeaways for all Organizations," the OPC raised a number of key elements and recommendations for all organizations subject to the federal *Personal Information and Electronic Documents Act* (PIPEDA), especially those that collect, use or disclose potentially sensitive personal information. We selected and addressed some of these key takeaways in the following sections:

### 1. Harm Extends Beyond Financial Harm

At the outset, the OPC interestingly noted that harm can extend beyond financial harm or impacts. Very often, when managing a breach of personal information or incident, organizations work under the assumption that unless the information is health information or information that can lead to fraud or identity theft, the information at stake is not sensitive. As the OPC pointed out, while financial impacts are highly visible, they do not represent the entire extent of possible harm. There are usually two main types of potential harms: *objective* types of harm, such as financial harm, physical harm or discrimination, and more *subjective* types of harm, which include an emotional component, such as humiliation, embarrassment, etc. The OPC notes that reputational harm (which may be linked to both subjective and objective types of harm) can be extremely damaging and may have long-term effects on an individual's ability to access and maintain employment, relationships or safety, and can be difficult to remediate. It is therefore essential that organizations carefully consider all risks of harm and properly assess and mitigate these risks.

## 2. Safeguards Supported by a Coherent and Adequate Governance Framework

With respect to safeguards, many businesses and organizations put their focus on technology, leaving behind other important issues such as governance and corporate culture. As the OPC noted, in order to meet their obligations under PIPEDA, organizations that hold large amounts of personal information must have safeguards appropriate to, among other factors, the sensitivity and amount of information collected. While technological safeguards are important, they should be supported by an adequate information security governance framework in order to ensure that practices are appropriate with regards to the risks. This can be done by implementing policies and procedures, but also by way of employee training and by ensuring that practices are consistently understood and effectively implemented. In the case of ALM, the OPC concluded that the lack of such a governance framework was an "unacceptable shortcoming" that "failed to prevent multiple security weaknesses."

## 3. Charging a Fee for the Deletion of Personal Information

ALM's practice, prior to the security breach, was to charge a $19 fee for the "full deletion" of user profile information. While PIPEDA does not expressly prohibit the inclusion of a fee in order to have personal information deleted from an organization's databases, the OPC interestingly determined that there will be a high bar for the imposition of such a barrier to the exercise of an individual's privacy rights. More specifically, the OPC mentioned that the reasonableness of such a fee would have to be evaluated in light of factors such as the actual cost to the organization relative to the fee charged, as well as the likely influence it would have on the individual's decision on whether to withdraw consent. Moreover, even in cases where such a fee is reasonable, it would have to be clearly and conspicuously communicated prior to an individual providing consent. We rarely see organizations discussing this aspect in their privacy policy, so this takeaway will be useful for all organizations that may consider charging a fee for deletion of personal information.

## 4. Retaining Information Contained in Inactive or Deactivated Profiles

ALM's practice was to keep all the information contained in inactive or deactivated profiles indefinitely, in case an individual wished to reactivate their profile in the future. This was done despite the fact that 99.9% of ALM users who did reactivate their account did so within 29 days of deactivation. The OPC's takeaway makes it clear that organizations should have a data retention practice aligned with the documented typical or standard behaviour of their users. In other words, the retention policies should be based on a demonstrable rationale and timeline. For instance, it may potentially be reasonable to retain data for a longer period but only if it can be demonstrated that users will often come back within the relevant period of time, that users have been adequately informed of this practice prior to providing consent and signing up for the service, etc.

## 5. Email Verification

Upon subscription, ALM required that all registrants provide an email address. However, ALM did not verify the authenticity of the email addresses provided by the registrants. In this respect, the OPC mentioned that this lack of email address verification created unnecessary reputational risks for non-users – allowing, for instance, the creation of a potentially reputation-damaging fake profile using a real email address. Following the

incident, non-users whose email addresses may have been released by the hacker and connected with ALM may be harmed and also have a claim against the organization for maintaining their personal information without their consent. This is a clear reminder that organizations that manage sensitive data and collect email addresses should implement an email verification process. It also highlights the risks for an organization of maintaining information which is not necessary, in breach of the data minimization principle.

### 6. Fake or Misleading Seals or Icons

Finally, many businesses display a seal or icon confirming or praising a certain level of quality or security. For instance, ALM was displaying, at the time of the breach, a fabricated "Trusted Security" icon, giving false assurances about the organization's security practices. The OPC observed in this respect that false or misleading statements, including fake or misleading seals or icons, may impact the validity of the consent obtained from users, as it may create false assurances which may materially influence an individual's decision to use a particular service.

### Conclusion

Many businesses and organizations may initially not feel concerned with the Ashley Madison security breach, given that they do not manage personal information which is as sensitive as information about users interested in extramarital affairs. However, the takeaways and recommendations contained in the OPC report apply to all organizations. The OPC report sheds light on a number of issues affecting all businesses and organizations, such as the importance of taking the risk of subjective and reputational harm into account; the need to implement safeguards supported by an adequate information security governance framework; the risks associated with charging a fee for the deletion of user profile information; the issues pertaining to the long-term retention of information contained in inactive or deactivated profiles; the importance of email verification; and the impact of false or misleading seals, icons or statements on the validity of consent.

Expertise

Cybersecurity, Privacy & Data Protection

## BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

**blg.com**

## BLG Offices


**Calgary**

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

**Ottawa**

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

**Vancouver**

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

**Montréal**

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

**Toronto**

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749