Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Australian Government
Office of the Australian Information Commissioner

Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner and Acting Australian Information Commissioner

Contents

Summary

1. Avid Life Media Inc. (ALM)[1] is a company that operates a number of adult dating websites. The largest website operated by ALM is Ashley Madison, which is targeted at people seeking a discreet affair. ALM is headquartered in Canada, but its websites have a global reach, with users in over 50 countries, including Australia.

2. On 15 July 2015, a person or group identifying itself as 'The Impact Team' announced that it had hacked ALM. The Impact Team threatened to expose the personal information of Ashley Madison users unless ALM shut down Ashley Madison and another of its websites, Established Men. ALM did not agree to this demand. On 20 July 2015, following media reports and after an invitation from the Office of the Privacy Commissioner of Canada (OPC), ALM voluntarily reported details of the breach to the OPC. Subsequently, on 18 and 20 August 2015, The Impact Team published information it claimed to have stolen from ALM, including the details of approximately 36 million Ashley Madison user accounts. The compromise of ALM's security by The Impact Team, together with the subsequent publication of compromised information online, is referred to in this report as 'the data breach'.

3. Given the scale of the data breach, the sensitivity of the information involved, the impact on affected individuals, and the international nature of ALM's business, the Office of the Australian Information Commissioner (OAIC) and the OPC jointly investigated ALM's privacy practices at the time of the data breach. The joint investigation was conducted in accordance with the Australian *Privacy Act 1988* (Australian Privacy Act) and the Canadian *Personal Information Protection and Electronic Documents Act* (PIPEDA). The collaboration was made possible by the OAIC and OPC's participation in the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Enforcement Arrangement and pursuant to ss 11(2) and 23.1 of PIPEDA and s 40(2) of the Australian Privacy Act.

4. The investigation initially examined the circumstances of the data breach and how it had occurred. It then considered ALM's information handling practices that may have affected the likelihood or the impact of the data breach. For clarity, this report makes no conclusions with respect to the cause of the data breach itself. The investigation assessed those practices against ALM's obligations under PIPEDA and the Australian Privacy Principles (APPs) in the Australian Privacy Act.

5. The primary issue under consideration was the adequacy of the safeguards ALM had in place to protect the personal information of its users. Although ALM's security was compromised by The Impact Team, a security compromise does not necessarily point to a contravention of PIPEDA or the Australian Privacy Act. Whether a contravention occurred depends on whether ALM had, at the time of the data breach:

    - for PIPEDA: implemented safeguards appropriate to the sensitivity of the information it held; and

[1] On 12 July 2016, Avid Life Media announced that it would be rebranded as Ruby Corp. See Avid Life Media, 'Avid Life Media Rebrands as ruby', 12 July 2016, available at <http://media.ashleymadison.com/avid-life-media-rebrands-as-ruby/>. The company will simply be referred to as ALM throughout this report in order to avoid confusion.

- for the Australian Privacy Act: taken such steps as were reasonable in the circumstances to protect the personal information it held.

6. The investigation also considered the following related information handling practices of ALM:

   - ALM's practice of retaining personal information of users after profiles had been deactivated or deleted by users, and when profiles were inactive (that is, had not been accessed by the user for an extended period of time);
   - ALM's practice of charging users to "fully delete" their profiles;
   - ALM's practice of not confirming the accuracy of user email addresses before collecting or using them; and
   - ALM's transparency with users about its personal information handling practices.

7. The investigation identified a number of contraventions of the APPs and PIPEDA.

8. Although ALM had a range of personal information security protections in place, it did not have an adequate overarching information security framework within which it assessed the adequacy of its information security. Certain security safeguards in some areas were insufficient or absent at the time of the data breach.

9. The findings of this report include important lessons for other organizations that hold personal information. The most broadly applicable lesson is that it is crucial for organizations that hold personal information electronically to adopt clear and appropriate processes, procedures and systems to handle information security risks, supported by adequate expertise (internal or external). This is especially the case where the personal information held includes information of a sensitive nature that, if compromised, could cause significant reputational or other harms to the individuals affected. Organizations holding sensitive personal information or a significant amount of personal information, as was the case here, should have information security measures including, but not limited to:

   - a security policy(cies);
   - an explicit risk management process that addresses information security matters, drawing on adequate expertise; and
   - adequate privacy and security training for all staff.

10. It is not sufficient for an organization such as ALM, or any organization that holds large amounts of personal information of a sensitive nature, to address information security without an adequate and coherent governance framework.

11. The OAIC and OPC provided a number of recommendations for ALM to follow to ensure it addressed the issues discussed in this report and brings itself into compliance with PIPEDA and the Australian Privacy Act with respect to those issues.

12. The Privacy Commissioner of Canada has accepted a compliance agreement, and the Acting Australian Information Commissioner has accepted an enforceable undertaking, from ALM. In accordance with these agreements ALM will be required to take significant additional steps to

address the issues identified in this report to protect the privacy of individuals, some of which have already been initiated by ALM.

Overview of investigation

Background

13. ALM is a private company, incorporated in Canada, which operates a number of adult dating websites. Each ALM website is targeted at a particular group. The websites operated by ALM are:

    - Ashley Madison, targeted at people seeking to participate in an affair;
    - Cougar Life, targeted at mature women seeking younger men (and vice versa);
    - Established Men, targeted at mature men seeking younger women (and vice versa); and
    - Man Crunch, targeted at men seeking men.

14. ALM has advised that Ashley Madison is its most visited website, hosting approximately 36 million user profiles at the time of the data breach, and that it has significant operating revenues, which in 2014 was in excess of US$100 million. At the time of the data breach, ALM employed around 100 staff, the majority of which were based at its headquarters in Toronto.[2]

The data breach

15. On 12 July 2015, ALM information technology employees detected unusual behaviour in ALM's database management system. This suggested to the ALM employees that an unauthorized access to the system was taking place. ALM took immediate steps to attempt to terminate the attacker's access to its systems.

16. On 13 July 2015, a notice appeared on computers being used by ALM customer service employees. The notice was purportedly from the attacker (who called itself 'The Impact Team'), and stated that ALM had been hacked. The notice said that, unless ALM shut down the Ashley Madison and Established Men websites, The Impact Team would publish stolen data online. On 19 July 2015, The Impact Team published notices on the internet announcing the attack and repeating the ultimatum that it had given to ALM.

17. ALM did not accede to the ultimatum and on 18 and 20 August 2015 a large number of files were posted online. The files contained database files taken from the Ashley Madison database and files taken from ALM's corporate network. The corporate information published included emails, source code and other business documents belonging to ALM. The Ashley Madison database files included details fromapproximately 36 million user accounts.

[2] Organisation chart provided by ALM management, October 2015.

User personal information affected in the data breach

18. The information published by the attacker fell into three main categories:[3]

    - **Profile information** that users entered to describe themselves, and the types of experiences they were looking for on the Ashley Madison website. This included user name, zip/postal code, relationship status, gender, height, weight, body type, ethnicity and date of birth, among other information. The profile information also included a number of optional fields, including checkboxes and free text fields (for example, 'My Intimate Desires', 'My Perfect Match', 'My Personal Interests' and 'My Limits Are') to be completed by users.
    - **Account information** used to facilitate access to the Ashley Madison service. This included information such as email addresses provided during account sign up, security questions and answers and hashed passwords.
    - **Billing information** for a subset of users who made purchases on the Ashley Madison website. The information included users' real names, billing addresses, and the last four digits of credit card numbers[4]. The content and formatting of the billing information published by the attacker strongly suggests that this information, some of which ALM retained in encrypted form, was obtained from a payment processor used by ALM, rather than directly from ALM - possibly through the use of compromised ALM credentials.[5]

19. ALM's forensic analysis was unable to determine the full extent of the access gained by the hackers, in part because the hackers were able to escalate their permissions to administrator level and erase logs that might have contained indicators of their activities. ALM told the investigation team, and affected individuals through notification emails, that apart from full payment card numbers, which were not generally stored by ALM, '…any other information that website visitors provided through AshleyMadison.com may have been acquired by the hacker.' This could have included users' photos, their communications with each other and ALM staff, and other information, in addition to the categories of information described above.

Post-incident response

20. After becoming aware of the compromise of its systems on 12 July 2015, ALM took steps to contain the data breach as quickly as possible, and to improve the security of its systems. After user data was posted online in August 2015, ALM took further steps striving to minimize the impact on affected individuals and on ALM's business.

21. On the same day it became aware of the attack, ALM took immediate steps to restrict the attacker's access to its systems, including temporarily shutting down its virtual private network (VPN) remote access server. Immediately after confirming that an attack had occurred on 13 July

---

[3] The content of the data dump was confirmed by analysis conducted by the Technology Analysis Unit of the OPC.

[4] A small number of full credit card numbers were contained in the published data. However, this information was only stored in the database due to user error, specifically, users placing credit card numbers into an incorrect free-text field.

[5] During discussions with the investigation team, ALM said that they speculated that the attackers may have gained access to the billing information by using the compromised ALM credentials to gain inappropriate access to these records held by one of their payment processors.

2015, ALM engaged a cybersecurity consultant to assist it in responding to the incident and to investigate the hacking attack, eliminate any continuing unauthorized intrusions and provide recommendations for strengthening ALM security.

22. On 20 July and 18 August 2015, ALM issued press releases confirming that a data breach had occurred. ALM established a dedicated telephone line and an email inquiry facility to allow affected users to contact ALM about the data breach. It later provided direct written notification by email to users in certain countries around the world, including 1.03 million in Canada, and 0.67 million in Australia. ALM also responded to requests by the OPC and OAIC to provide additional information about the data breach on a voluntary basis prior to the initiation of this joint investigation.

23. ALM subsequently took significant measures to improve its information security. In October 2015, ALM hired an experienced Chief Information Security Officer (who replaced the previous Director of Security in place from early to mid 2015), who now reports directly to the ALM CEO (with a 'dotted line' to the ALM Board). In October 2015 it engaged Deloitte to assist it in improving its information security practices, beginning with a comprehensive review of ALM's security framework, followed by the creation of documented policies and procedures. This also included additional training for staff, and other measures in advance of receiving the recommendations made in this report.

24. ALM has made significant efforts to limit the dissemination of the stolen information online. ALM sent takedown notices to all sites it was aware of that hosted messages from The Impact Team, ALM corporate data, or the database file. Although not all websites ALM contacted took down information as requested, many did. As such, these actions reduced the spread of the information online, and made it more difficult for casual internet users to locate information about people whose personal information was compromised in the data breach.

25. ALM fully cooperated with the joint OPC and OAIC investigation, providing access to information and staff as requested.

Information considered in preparing this report

26. In reaching the conclusions set out in this report, the investigation team considered information including the following:

    - Interviews conducted with the following ALM personnel:
        - Chief Operating Officer;
        - General Counsel;
        - Vice President, Technology Operations; and
        - Vice President, Support & Service.
    - A walkthrough of the Ashley Madison website provided by ALM staff;
    - Data breach notifications made by ALM to the OPC and OAIC;
    - Written responses from ALM to questions posed by the OAIC and OPC;
    - The terms and conditions of Ashley Madison and ALM's other websites, as they were prior to the data breach, and as they were at 27 October 2015;

- Payment Card Industry Data Security Standard (PCI-DSS) incident and compliance reports;
- Information provided to ALM by a cybersecurity consultant;
- ALM's information technology operational procedures; and
- ALM's information security and privacy training material.

27. This report was further informed by analysis conducted by the OPC's Technology Analysis Unit of the information and documents above, including corroboration against data points posted on the Internet by the attackers, and corroboration of the Ashley Madison website user experience.

Jurisdiction and decisions to investigate

PIPEDA

28. The Privacy Commissioner of Canada, having been satisfied that reasonable grounds existed to investigate this matter, and having jurisdiction over ALM, headquartered in Ontario, Canada, commenced a Commissioner-initiated complaint under section 11.(2) of PIPEDA and so advised ALM on 21 August 2015.

Australian Privacy Act

29. ALM is an organisation as defined in s 6C(1)(b) of the Australian Privacy Act, being a body corporate that is not a small business operator. Although ALM is headquartered in Canada, the Australian Privacy Act extends to an act done, or practice engaged in, outside Australia by an organisation where that organisation has an 'Australian link' (s 5B(1A)).

30. An organisation or small business operator has an Australian link where it is:

- an Australian citizen or a person whose continued presence in Australia is not subject to a legal time limitation;
- a partnership formed, or a trust created, in Australia or an external Territory;
- a body corporate incorporated in Australia or an external Territory; or
- an unincorporated association that has its central management and control in Australia or an external Territory (s 5B(2)).

31. None of these categories apply to ALM. However, an organisation that does not fall within one of those categories will also have an Australian link where:

- it carries on business in Australia or an external Territory (s 5B(3)(b)); and
- it collected or held personal information in Australia or an external Territory, either before or at the time of the act or practice (s 5B(3)(c)).

32. Although ALM does not have a physical presence in Australia, it conducts marketing in Australia, targets its services at Australian residents, and collects information from people in Australia. ALM

has advertised in Australia, and the Ashley Madison website at the time of the breach had pages targeted specifically at Australian users.[6] For this reason, it carries on business in Australia.

33. Personal information is collected 'in Australia' for the purpose of s 5B(3)(c) of the Australian Privacy Act, if it is collected from an individual who is physically present in Australia or an external Territory, regardless of where the collecting entity is located or incorporated. This applies even if the website is owned by a company that is located outside of Australia or that is not incorporated in Australia.[7] By gathering information about Australian users of the ALM website, ALM collects personal information in Australia.

34. The OAIC is satisfied that ALM is an organisation with an Australian link, and as such, under s 15 of the Australian Privacy Act is prohibited from doing an act, or engaging in a practice, that breaches an Australian Privacy Principle.

35. Under s 40(2) of the Act, the Australian Information Commissioner may, on his own initiative, investigate an act or practice if it may be an interference with the privacy of an individual or a breach of APP 1, and the Commissioner thinks it is desirable that the act or practice be investigated. The Commissioner notified ALM of his decision to conduct an investigation under s 40(2) on 21 August 2015.

36. In the interests of avoiding duplication of efforts, and advancing expeditiously an investigation of the issues in this matter, the OPC and OAIC conducted their investigations jointly.

Status of recommendations and report

37. This report identifies a number of contraventions of PIPEDA and the Australian Privacy Act, and provides recommendations for ALM to take to address these contraventions. ALM has agreed to implement all of the recommendations contained in this report.

38. Section 13(1)(a) of PIPEDA requires the Privacy Commissioner of Canada to prepare a report that contains the Commissioner's findings and recommendations. On the basis of our investigation and ALM's agreement to implement the recommendations, for the matters raised in the subsequent sections of this report: 'Information Security', 'Indefinite retention and paid deletion of user accounts', 'Accuracy of email addresses', and 'Transparency with users' - the Commissioner finds the matters well-founded and conditionally resolved.

39. Section 33E permits the Australian Information Commissioner to accept an enforceable undertaking from an organization that it will take certain steps to comply with the Privacy Act or to avoid an interference with privacy. ALM has offered the Commissioner an undertaking to address the issues identified in this report.

---

6 The webpage https://www.ashleymadison.com/landers/australia_dating (accessed 20 August 2015) promotes Australian media coverage of the Ashley Madison website, and states 'With more than 460,000 members in Australia, Ashley Madison is the final destination for married women and married men looking to maintain their anonymity while looking to have an affair.'

7 See Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth), p 218.

Compliance Agreement and Enforceable Undertaking

40. Our Offices have a continuing interest in ensuring that ALM implements the measures needed to bring it into full compliance with the Acts. As such, our Offices will be closely monitoring the organization's implementation of our recommendations and have entered into:

    a) a Compliance Agreement (OPC) with ALM pursuant to subsection 17.1(1) of PIPEDA; and

    b) an Enforceable Undertaking (OAIC) pursuant to s 33E of the Australian Privacy Act.

41. Our Offices appreciate ALM's further demonstration of its commitment to addressing our concerns through the Compliance Agreement and Enforceable Undertaking.

Information security

Requirement to safeguard personal information

42. Organizations are required to protect the personal information they hold. Principle 4.7 in PIPEDA requires that personal information be protected by safeguards appropriate to the sensitivity of the information, and Principle 4.7.1 requires security safeguards to protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification.

43. Similarly, APP 11.1 in the Australian Privacy Act requires entities to take such steps as are reasonable in the circumstances to protect personal information held by the entity from misuse, interference and loss, as well as unauthorized access, modification or disclosure. Under both pieces of legislation, the level of protection required varies depending on the circumstances, including the nature and sensitivity of the information held.[8]

44. For PIPEDA, a meaningful assessment of the required level of safeguards for any given personal information must be context based, commensurate with the sensitivity of the data and informed by the potential risk of harm to individuals from unauthorized access, disclosure, copying, use or modification of the information. This assessment should not focus solely on the risk of financial loss to individuals due to fraud or identity theft, but also on their physical and social well-being at stake, including potential impacts on relationships and reputational risks, embarrassment or humiliation.

45. Similarly, for the Australian Privacy Act, in assessing the 'circumstances' referred to in APP 11.1, it is relevant to consider the potential risk of harm to individuals should the security of the information in question be compromised.

46. In this case, a key risk to individuals is the possibility of reputational harm. Harm to reputation is a potentially high-impact risk as it can affect an individual's long term ability to access and maintain employment, critical relationships, safety, and other necessities depending on the nature of the information held. In today's online environment, once information affecting a person's reputation is disclosed, correct or not, it can continue to affect them indefinitely.

47. ALM provides online adult dating services, and as such collects, holds and uses sensitive information[9] about its users, including information that reveals the sexual practices, preferences and fantasies of those users. Furthermore, Ashley Madison is a website designed for people who are seeking to engage in an affair, an activity where discretion is expected and paramount. As such, even information that in isolation might be regarded as innocuous in a different context (such as

---

[8] See Principle 4.7.2 of PIPEDA. See also paragraph 11.7 of the Australian Privacy Principles guidelines, which sets out factors that are often relevant when assessing the extent of 'reasonable steps' required under APP 11.

[9] 'Sensitive information' is defined in s 6 the Australian Privacy Act by the inclusion of a list of 13 specified categories of information. This includes 'information or an opinion about an individual's … sexual orientation or practices', which would cover some of the information held by ALM. In the following paragraphs reference is made to information of a 'sensitive nature' or the 'sensitivity' of information, as this is a relevant consideration for PIPEDA and when assessing what 'reasonable steps' are needed to secure personal information. This is not intended to indicate that the information is 'sensitive information' as defined in s 6 of the Australian Privacy Act, unless otherwise noted.

names or email addresses) can take on a more sensitive nature when connected with the Ashley Madison website.[10]

48. Following the data breach, the OPC and OAIC became aware both directly (from affected individuals) and indirectly (by way of media reports) of extortion attempts against individuals whose information was compromised as a result of the data breach. In some cases, affected individuals received email messages threatening to disclose their involvement with Ashley Madison to family members or employers if they failed to make a payment in exchange for silence. The very existence and form of such extortion attempts further illustrates the highly sensitive nature of this information from a reputational perspective.

49. Not all ALM users would be identifiable from the information held by ALM. For instance, some users who did not provide their real name for the purpose of purchasing credits, who used an email address that did not identify them, and did not disclose other personal information, such as photos, may not have been identifiable. However, ALM could have reasonably foreseen that the disclosure of the information held by it to an unauthorized person, or to the world at large, could have significant adverse consequences for the many people who could be identified. Information on the Ashley Madison website, including the mere association of an individual's identity with a user account on the website, is a significant consideration given the potential harm that disclosure of the information may cause.

50. By its own actions, ALM was evidently well aware of the sensitivity of the information it held. Discretion and security were marketed and highlighted to its users as a central part of the service it offered and undertook to provide, in particular on the Ashley Madison website. In an interview conducted with the OPC and OAIC on 29 October 2015, a member of ALM's senior executive team stated 'the protection of our customer's confidence is at the core of our brand and our business'. This internal view was explicitly reflected in the marketing communications directed by ALM towards its users.

51. At the time of the data breach, the front page of the Ashley Madison website included a series of trust-marks which suggested a high level of security and discretion (see Figure 1 below). These included a medal icon labelled 'trusted security award', a lock icon indicating the website was 'SSL secure' and a statement that the website offered a '100% discreet service'. On their face, these statements and trust-marks appear to convey a general impression to individuals considering the use of ALM's services that the site held a high standard of security and discretion and that individuals could rely on these assurances. As such, the trust-mark and the level of security it represented, could have been material to their decision whether or not to use the site.

52. When this view was put to ALM in the course of this investigation, ALM noted that the Terms of Service warned users that security or privacy information could not be guaranteed, and if they accessed or transmitted any content through the use of the Ashley Madison service, they did so at their own discretion and at their sole risk. However, this statement cannot absolve ALM of its legal obligations under either Act.

---

[10] PIPEDA Principle 4.3.4 gives as an example that while the contact information of subscribers to a newsmagazine would generally not be considered sensitive, the same information for subscribers of a special-interest magazine may be.

Figure 1: Trust-marks on the Ashley Madison Australian website front page prior to data breach

53. Considering the nature of the personal information collected by ALM, and the type of services it was offering, the level of security safeguards should have been commensurately high in accordance with PIPEDA Principle 4.7.

54. Under the Australian Privacy Act, organizations are obliged to take such 'reasonable' steps as are required in the circumstances to protect personal information. Whether a particular step is 'reasonable' must be considered with reference to the organization's ability to implement that step. ALM advised the OPC and OAIC that it had gone through a rapid period of growth leading up to the time of the data breach, and was in the process of documenting its security procedures and continuing its ongoing improvements to its information security posture at the time of the data breach.

55. For the purpose of APP 11, when considering whether steps taken to protect personal information are reasonable in the circumstances, it is relevant to consider the size and capacity of the organization in question. As ALM submitted, it cannot be expected to have the same level of documented compliance frameworks as larger and more sophisticated organizations. However, there are a range of factors in the present circumstances that indicate that ALM should have implemented a comprehensive information security program. These circumstances include the quantity and nature of the personal information ALM held, the foreseeable adverse impact on individuals should their personal information be compromised, and the representations made by ALM to its users about security and discretion.

Requirement to establish appropriate practices, procedures and systems

56. In addition to the obligation to take reasonable steps to secure user personal information, APP 1.2 in the Australian Privacy Act requires organizations to take reasonable steps to implement practices, procedures and systems that will ensure the entity complies with the APPs. The purpose of APP 1.2 is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems to meet its privacy obligations.

57. Similarly, PIPEDA Principle 4.1.4 (Accountability) dictates that organizations shall implement policies and practices to give effect to the Principles, including implementing procedures to protect personal information and developing information to explain the organization's policies and procedures.

58. Both APP 1.2 and PIPEDA Principle 4.1.4 require organizations to establish business processes that will ensure that the organization complies with each respective law. As well as considering the specific safeguards ALM had in place at the time of the data breach, the investigation considered the governance framework ALM had in place to ensure that it met its privacy obligations.

The data breach

59. ALM became aware of the incident on 12 July 2015 and engaged a cybersecurity consultant to assist it in its investigations and response on 13 July 2015. The description of the incident set out below is based on interviews with ALM personnel and supporting documentation provided by ALM.

60. It is believed that the attackers' initial path of intrusion involved the compromise and use of an employee's valid account credentials. The attacker then used those credentials to access ALM's corporate network and compromise additional user accounts and systems. Over time the attacker accessed information to better understand the network topography, to escalate its access privileges, and to exfiltrate data submitted by ALM users on the Ashley Madison website.

61. The attacker took a number of steps to avoid detection and to obscure its tracks. For example, the attacker accessed the VPN network via a proxy service that allowed it to 'spoof' a Toronto IP address. It accessed the ALM corporate network over a long period of time in a manner that minimized unusual activity or patterns in the ALM VPN logs that could be easily identified. Once the attacker gained administrative access, it deleted log files to further cover its tracks. As a result, ALM has been unable to fully determine the path the attacker took. However, ALM believes that the attacker had some level of access to ALM's network for at least several months before its presence was discovered in July 2015.

62. The methods used in the attack suggest it was executed by a sophisticated attacker, and was a targeted rather than opportunistic attack.

Safeguards in place at the time of the data breach

63. The investigation considered the safeguards that ALM had in place at the time of the data breach to assess whether ALM had met the requirements of PIPEDA Principle 4.7 and APP 11.1. ALM provided OPC and OAIC with details of the physical, technological and organizational safeguards in place on its network at the time of the data breach. According to ALM, key protections included:

- **Physical safeguards:** Office servers were located and stored in an isolated, locked room with access limited by keycard to authorized employees. Production servers were stored in a cage at ALM's hosting provider's facilities, with entry requiring a biometric scan, an access card, photo ID, and a combination lock code.
- **Technological safeguards**: Network protections included network segmentation, firewalls, and encryption on all web communications between ALM and its users, as well as on the channel through which credit card data was sent to ALM's third party payment processor. All external access to the network was logged. ALM noted that all network access was via VPN, requiring authorization on a per user basis requiring authentication through a 'shared secret' (see further detail in paragraph 72). Anti-malware and anti-virus software were installed. Particularly sensitive information, specifically users' real names, addresses and purchase information, was encrypted, and internal access to that data was logged and monitored (including alerts on unusual access by ALM staff). Passwords were hashed using the BCrypt algorithm (excluding some legacy passwords that were hashed using an older algorithm).
- **Organizational safeguards:** ALM had commenced staff training on general privacy and security a few months before the discovery of the incident. At the time of the breach, this training had been delivered to C-level executives, senior IT staff, and newly hired employees, however, the

large majority of ALM staff (approximately 75%) had not yet received this training. In early 2015, ALM engaged a Director of Information Security to develop written security policies and standards, but these were not in place at the time of the data breach. It had also instituted a bug bounty program in early 2015 and conducted a code review process before making any software changes to its systems. According to ALM, each code review involved quality assurance processes which included review for code security issues.

64. The OAIC and OPC sought, in particular, to understand the protections in place relevant to the path of attack, which was compromised VPN credentials, used to access ALM's systems undetected for a significant period of time. Specifically, the investigation team sought to understand ALM's related security policies and practices, how ALM determined that those policies and practices were appropriate to the relevant risks, and how it ensured those policies and practices were properly implemented.

Policies

65. At the time of the incident, ALM did not have documented information security policies or practices for managing network permissions. Having documented security policies and procedures is a basic organizational security safeguard, particularly for an organization holding significant amounts of personal information. Making informational policies and practices explicit provides clarity about expectations to facilitate consistency, and helps to avoid gaps in security coverage. It also sends key signals to employees about the importance placed on information security. Furthermore, such security policies and processes need to be updated and reviewed based on the evolving threat landscape, which would be very challenging if they are not formalized in some manner.

66. In early 2015 ALM engaged a full time Director of Information Security, who, at the time of the breach, was in the process of developing written security procedures and documentation. However, this work was incomplete at the time the data breach was discovered. ALM said that although it did not have documented information security policies or procedures in place, undocumented policies did exist, and were well understood and implemented by the relevant employees.

67. However, the investigation team found critical gaps in security coverage indicative of the absence of appropriate policies and practices. For instance, security policies and procedures should cover both preventive and detective measures. According to information provided, ALM had not implemented a number of commonly used detective countermeasures that could facilitate detection of attacks or identify anomalies indicative of security concerns. While such systems would not necessarily have detected intrusions such as the one by the attacker, they are important lines of defense that could potentially limit the adverse impact of attacks.

68. ALM did have some detection and monitoring systems in place, but these were focused on detecting system performance issues and unusual employee requests for decryption of sensitive user data. ALM had not implemented an intrusion detection system or prevention system and did not have a security information and event management system in place, or data loss prevention monitoring. VPN logins were tracked and reviewed on a weekly basis, however unusual login behaviour, which could give indicators of unauthorized activity, was not well monitored. For instance, it was only in the course of investigating the current incident that ALM's third party cybersecurity consultant discovered other instances of unauthorized access to ALM's systems,

using valid security credentials, in the weeks immediately preceding its discovery of the breach in question. This further reinforces our view that ALM was not adequately monitoring its systems for indications of intrusion or other unauthorized activity.

Risk Management

69. At the time of the breach, ALM did not have a documented risk management framework guiding how it determined what security measures would be appropriate to the risks it faced. Conducting regular and documented risk assessments is an important organizational safeguard in and of itself, which allows an organization to select appropriate safeguards to mitigate identified risks and reassess as business and threat landscapes change. Such a process should be supported by adequate external and/or internal expertise, appropriate to the nature and volume of personal information held and the risks faced.

70. ALM claimed that although no risk management framework was documented, its security program was based on an assessment of potential threats. ALM did undertake patch management and quarterly vulnerability assessments as required for an organization to accept payment card information (to be PCI-DSS compliant). However, it could not provide evidence that it had undertaken any structured assessment of the overall threats facing it, or that it had assessed its information security framework through standard exercises such as internal or external audits or evaluations.

71. With respect to the adequacy of ALM's decision-making on selecting security measures, ALM noted that prior to the breach, it had, at one point, considered retaining external cybersecurity expertise to assist in security matters, but ultimately elected not to do so. In early 2015 it engaged a full time Director of Information Security. However, despite this positive step, the investigation found some cause for concern with respect to decision making on security measures. For instance, as the VPN was a path of attack, the OAIC and OPC sought to better understand the protections in place to restrict VPN access to authorized users.

72. ALM advised that to access its systems remotely via VPN, a user would need: a username, a password, a 'shared secret' (a common passphrase used by all VPN users to access a particular network segment), the VPN group name, and the IP address of ALM's VPN server. The OPC and OAIC note that although users would need three pieces of information to be authenticated, in fact, these pieces of information provided only a single factor of authentication ('something you know'). Multi-factor authentication is commonly understood to refer to systems that control access on the basis of two or more different factors.[11] Different factors of authentication include: something you *know*, such as a password or shared secret; something you *are*, namely, biometric data[12] such as a

---

[11] See Australian Cyber Security Operations Centre (2014) 'Multi-factor authentication', available online at <http://www.asd.gov.au/publications/protect/multi_factor_authentication.htm>; OAIC (2015) 'Guide to Securing Personal Information', available online at <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>.

[12] Care should be taken to weigh the privacy risks and benefits if considering the use of biometrics as a factor of authentication. We note that the use of biometrics for authentication should be reserved for only those cases where the circumstances warrant it, based on a contextual and proportionate assessment of the risks involved. These include not only the risks that a biometric as an authentication measure seeks to mitigate, but also the attendant risks associated with the use of the biometric itself. For further information on the use of

fingerprint or retina scan; and something you *have*, such as a physical key, login device or other token. Since the incident, ALM has implemented a second factor of authentication for VPN remote access in the form of 'something you have'.

73. Multi-factor authentication is a commonly recommended industry practice for controlling remote administrative access given the increased vulnerability of a single vs. multi-factor authentication. Given the risks to individuals' privacy faced by ALM, ALM's decision not to implement multi-factor authentication for administrative remote access in these circumstances is a significant concern.

Training and Implementation

74. Security policies and practices are only effective when properly and consistently implemented and followed by employees. For this reason, in all but the smallest organizations handling personal information, formal training on information security and privacy responsibilities is key to ensuring that obligations are consistently understood and acted upon by employees. At the time of the breach, a security training program had recently been developed, but had only been delivered to approximately 25% of staff - principally new hires, C-level executives and senior IT staff. ALM claimed that although most employees had not been given the security training program (including certain IT staff), and although the relevant policies and procedures were not documented, employees were aware of their obligations where these obligations were relevant to their job functions. However, the investigation found that this was not uniformly the case.

75. Information provided by ALM in the wake of the breach highlighted several other instances of poor implementation of security measures, particularly, poor key and password management practices. These include the VPN 'shared secret' described above being available on the ALM Google Drive, meaning that anyone with access to any ALM employee's drive on any computer, anywhere, could have potentially discovered the shared secret. Instances of storage of passwords as plain, clearly identifiable text in emails and text files were also found on the systems. In addition, encryption keys were stored as plain, clearly identifiable text on ALM systems, potentially putting information encrypted using those keys at risk of unauthorized disclosure. Finally, a server was found with an SSH key that was not password protected. This key would enable an attacker to connect to other servers without having to provide a password.

Findings

76. Prior to becoming aware that its systems had been compromised in July 2015, ALM had in place a range of security safeguards to protect the personal information it held. In spite of these safeguards, the attack occurred. The fact that security has been compromised does not necessarily mean there has been a contravention of either PIPEDA or the Australian Privacy Act. Rather, it is necessary to consider whether the safeguards in place at the time of the data breach were sufficient having regard to, for PIPEDA, the 'sensitivity of the information', and for the APPs, what steps were 'reasonable in the circumstances'.

77. As noted above, given the sensitivity of the personal information it held, the foreseeable adverse impact on individuals should their personal information be compromised, and the representations

---

biometrics see the OPC's 'Data at Your Fingertips: Biometrics and the Challenges to Privacy', available online at <https://www.priv.gc.ca/information/pub/gd_bio_201102_e.asp>. We are satisfied, in this case, that ALM's addition of a 'something you have' factor as a second factor of authentication is appropriate in this case.

made by ALM about security of its information systems, the steps ALM is required to take to comply with the security obligations in PIPEDA and the Australian Privacy Act are of a commensurately high level.

78. In this context, the Commissioners are of the view that ALM's security framework was lacking the following key elements:

    a) documented information security policies or practices, as a cornerstone of fostering a privacy and security aware culture including appropriate training, resourcing and management focus;

    b) an explicit risk management process - including periodic and pro-active assessments of privacy threats, and evaluations of security practices to ensure ALM's security arrangements were, and remained, fit for purpose; and

    c) adequate training to ensure all staff (including senior management) were aware of, and properly carried out, their privacy and security obligations appropriate to their role and the nature of ALM's business.

79. As such, the Commissioners are of the view that ALM did not have appropriate safeguards in place considering the sensitivity of the personal information under PIPEDA, nor did it take reasonable steps in the circumstances to protect the personal information it held under the Australian Privacy Act. Though ALM had some security safeguards in place, those safeguards appeared to have been adopted without due consideration of the risks faced, and absent an adequate and coherent information security governance framework that would ensure appropriate practices, systems and procedures are consistently understood and effectively implemented. As a result, ALM had no clear way to assure itself that its information security risks were properly managed. This lack of an adequate framework failed to prevent the multiple security weaknesses described above and, as such, is an unacceptable shortcoming for an organization that holds sensitive personal information or a significant amount of personal information, as in the case of ALM.

80. In addition to the lack of an adequate framework, in our view, the specific weaknesses (single factor authentication and poor key and password management practices) described in paragraphs 72 and 75 also individually and collectively constitute failures to take reasonable steps to implement appropriate security safeguards in the specific circumstances, given the volume and nature of the personal information held by ALM.

81. Both by not having and documenting an appropriate information security framework and by not taking reasonable steps to implement appropriate security safeguards, ALM contravened APP 1.2, APP 11.1 and PIPEDA Principles 4.1.4 and 4.7.

Recommendations for ALM

82. To address the above findings, the OPC and OAIC recommend that ALM:

    a) by 31 December 2016, conduct a comprehensive review of the protections it has in place to protect personal information;

    b) by 31 May 2017, augment its information security framework to an appropriate level and implement that framework;

c) by 31 May 2017, adequately document that framework and its information security processes generally;

d) take steps to ensure that staff are aware of and follow security procedures, including developing an appropriate training program and delivering it to all staff and contractors with network access (the Commissioners note that ALM has reported completion of this recommendation); and

e) by 31 July 2017, provide the OPC and OAIC with a report from an independent third party documenting the measures it has taken to come into compliance with the above recommendations or provide a detailed report from a third party, certifying compliance with a recognized privacy/security standard satisfactory to the OPC and OAIC.

Indefinite retention and paid deletion of user accounts

Requirement to destroy or de-identify personal information no longer required

83. Both PIPEDA and the Australian Privacy Act place limits on the length of time that personal information may be retained.

84. APP 11.2 states that an organization must take reasonable steps to destroy or de-identify information it no longer needs for any purpose for which the information may be used or disclosed under the APPs. This means that an APP entity will need to destroy or de-identify personal information it holds if the information is no longer necessary for the primary purpose of collection, or for a secondary purpose for which the information may be used or disclosed under APP 6.

85. Similarly, PIPEDA Principle 4.5 states that personal information shall be retained for only as long as necessary to fulfil the purpose for which it was collected. PIPEDA Principle 4.5.2 also requires organizations to develop guidelines that include minimum and maximum retention periods for personal information. PIPEDA Principle 4.5.3 states that personal information that is no longer required must be destroyed, erased or made anonymous, and that organizations must develop guidelines and implement procedures to govern the destruction of personal information.

86. ALM indicated during this investigation that profile information related to user accounts which have been deactivated (but not deleted), and profile information related to user accounts which have not been used for a prolonged period, is retained indefinitely.

87. Following the data breach, there were media reports that personal information of individuals who had paid ALM to delete their accounts was also included in the Ashley Madison user database published on the internet.

Requirement to delete an individuals' information on request by the individual

88. In addition to the requirement to not retain personal information once it is no longer required, PIPEDA Principle 4.3.8 states that an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice.[13]

89. Included in the personal information compromised by the data breach was the personal information of users who had deactivated their accounts, but who had not chosen to pay for the full delete of their profiles.

90. The investigation considered ALM's practice, at the time of the data breach, of retaining personal information of individuals who had either:

    a) not used their profiles for a prolonged period ('inactive' profiles);

    b) deactivated their profiles; or

    c) deleted their profiles.

    to determine whether ALM had contravened PIPEDA or the Australian Privacy Act.

[13] There is no analogous provision in the Australian Privacy Act.

91. Two issues are at hand. The first issue is whether ALM retained information about users with deactivated, inactive and deleted profiles for longer than needed to fulfil the purpose for which it was collected (under PIPEDA), and for longer than the information was needed for a purpose for which it could be used or disclosed (under the Australian Privacy Act's APPs).

92. The second issue (for PIPEDA) is whether ALM's practice of charging users a fee for the complete deletion of all of their personal information from ALM's systems contravenes the provision under PIPEDA's Principle 4.3.8 regarding the withdrawal of consent.

Practices at the time of the data breach

93. The Ashley Madison website offers two ways to close a user account. These are presented to users as a 'basic deactivation' and a 'full delete' option, and are described below. ALM advised that on its other websites only the basic deactivation option is available.

'Basic deactivation' of user profiles

94. The basic deactivation option is listed beside a banner that reads: 'Hide your profile from search'. It is followed by a note that says:

> *Hiding Your Profile Includes:*
>
> - *removal of profile from search results.*
>
> *Important: Your profile information and messages will be accessible to members you've communicated with.*

95. The basic deactivation option can be accessed by users for free, and is reversible if a user changes their mind and decides to return to Ashley Madison.

96. Following account deactivation, information associated with the account is retained indefinitely.

97. ALM explained that it retained information about deactivated profiles for two reasons. First, ALM said that it was necessary to retain user information to preserve 'header information' in messages that had been sent to other users. Each message sent to another user on Ashley Madison contains a 'header' with basic profile information about the sender. For the messages that the user had previously sent to other users to remain visible to those other users with full header details intact, it is necessary for ALM to keep the profile information of the sender to populate the message header. ALM linked this to email messages in an inbox having the 'from' information intact regardless of whether the person who sent the email is still using that email address. Second, ALM said that users who chose to deactivate their profile will often choose to reactivate their profile at a later date. By retaining information about deactivated profiles, ALM could provide a better customer experience for returning users.

98. ALM provided information about the number of users who had reactivated their accounts following deactivation. These figures indicated that of users who reactivated their accounts, 99.9% of these users did so within 29 days of deactivating their account.

Retention of inactive profiles

99. Profiles of users who have not used their accounts for a prolonged period ('inactive' profiles) are also retained indefinitely.

100. The Ashley Madison Terms and Conditions at the time of the breach indicated that ALM reserves the right to '…delete any of your accounts and all related information and files in such accounts…' without prior notice.

'Full delete' of user accounts

101. The 'full delete' option is listed beside a banner that reads: 'Delete your profile'. It is followed by a note that says:

> *Full Delete Removal Includes:*
>
> - *Removal of profile from search results*
> - *Removal of profile from the site*
> - *Removal of messages sent and received*
> - *Removal of messages from recipient's mailboxes including Winks & Gifts*
> - *Removal of site usage history and personally identifiable information from the site*
> - *Removal of photos*
>
> Note: It may take up to 48 hours for some traces of your profile to be fully removed.

102. ALM explained that the full delete option had been developed in response to user demand, and at significant expense. The full delete option was designed to provide an additional level of discretion for users who had decided to leave Ashley Madison. ALM stated that it was a technically difficult task to remove all traces of a user from its system. For example, it was difficult to remove sent messages from the inboxes of message recipients. ALM also indicated that there was a customer service cost associated with deleting accounts because ALM's customer service staff received inquiries from users who were confused when messages vanished from their inbox when the person they had been corresponding with decided to delete their account.

103. At the time of the data breach, ALM charged a fee to allow users to access the full delete service. The fee for Canadian users was C$19. At the time of the breach, neither the Ashley Madison Privacy Policy, nor the Ashley Madison Terms and Conditions contained a notification that a fee would be charged by ALM for individuals to delete their personal information. ALM has informed the OPC and OAIC that, following the data breach, it is not currently charging a fee for the full delete service.

104. At the time of the data breach, ALM's policy was that if a user purchased a full delete, their personal information was made inaccessible through the Ashley Madison website within 24 to 48 hours, but was retained by ALM for a further 12 months.

105. ALM clarified that due to an error, at the time of the data breach photos from deleted accounts had been moved to a non-user facing folder marked for future disposal, but had not actually been deleted after the 12 month period specified above. These photos may have been accessed by the

attacker. ALM has since removed all photos associated with users who selected full delete from this folder and corrected the underlying technical issue.

106. ALM stated that it retained information for use if a departing user fraudulently attempted to make a credit card 'chargeback', claiming they had not been an Ashley Madison user. This is a procedure by which a credit card user can claim that their credit card was used fraudulently to make a payment online and obtain a refund from the vendor.

107. Where a user claims a chargeback, it falls on ALM to demonstrate to the bank that the user did in fact use ALM's services. By retaining photos, account information, and usage history for a 12 month period, ALM would have information on hand to allow it to demonstrate to the individual's bank that the credit card payment was legitimate. ALM said that given the nature of its websites, it receives chargebacks that amount to a substantial monetary figure. Therefore, ALM needed to prevent fraudulent chargebacks, or would incur a significant cost.

108. At the time of the breach, the retention of information following a full delete was drawn to the attention of its users, at the time a full delete was purchased, but only after the user's payment had been accepted, when users were provided with a confirmation notice which said:

> *This notice confirms that Ad Profile number … has been successfully deleted from our system. Some information will be retained for 6-12 months due to legal and financial reasons after which it will be removed as well.*
> *…*
> *If you wish to correspond with our office regarding this notice, the privacy of your personal information or any other matter, please contact us.*

109. In its Terms and Conditions ALM also had the following language relating to its practice of retaining information to respond to fraudulent chargebacks in its terms and conditions:

> ***Credit Card Chargeback Policy***
>
> *We protect our business and credit card processors, banks and other institutions providing related services to use from fraudulent credit card chargebacks. A credit card chargeback is when the holder of a credit card disputes a charge with a credit card processor … . You understand and agree that in the event you attempt to create a fraudulent credit card chargeback, we will work with the relevant credit card processor, bank or other institution and law enforcement authorities to investigate the matter. Our assistance may include providing details about the profiles, card authentication and communications with or related to our Service or other users or members. …*

110. ALM presented statistics about chargebacks and their frequency. The majority of chargebacks occur within 3 months of purchase. This is followed by a steep drop-off in chargebacks, with the overwhelming majority (around 98%) occurring within 6 months from the date of purchase, around 2% occurring between 6-12 months after purchase, and 0.1% occurring more than 12 months after purchase.

Findings

Indefinite retention for deactivated accounts

111. Both PIPEDA and the Australian Privacy Act require that personal information only be retained so long as it is required. In the case of PIPEDA, this means for as long as necessary to fulfil the purpose for which the personal information was collected. In the case of the Australian Privacy Act, this is for so long as it may be used or disclosed for a purpose permitted by the APPs.

112. ALM has presented an explanation about why it retains user information following basic deactivation. It is conceivable that users would wish to return to the Ashley Madison (or other ALM) website after deactivation, and having their profile information on hand would make this easier.

113. That said, there is nothing in ALM's privacy policy or on its website that communicates to prospective and existing users the implications of a basic deactivation on the retention of personal information, and certainly not that information would continue to be held indefinitely by ALM (failing payment for the full delete option).

114. In our view, it is not reasonable that personal information of users whose accounts are deactivated is required to be kept *indefinitely*. The figures provided by ALM indicated that vast majority of users who reactivated their accounts did so after an extremely short period of time (99.9% within 29 days), and most chargeback requests from credit card providers were received within 12 months. These figures did not provide any justification for indefinite retention.

115. Profile information collected from ALM users is gathered for the primary purpose of providing an online dating service. After a certain period of time following basic deactivation, it is highly unlikely the user will return to ALM's website, and therefore the personal information of users is no longer needed for that purpose. At that point, and absent any other legitimate purpose for retaining the personal information in question, ALM must destroy or de-identify it.

116. As such, although ALM is entitled to retain information following a basic deactivation for a reasonable period to allow for the return of users to its websites, ALM's practice of *indefinite* retention contravenes PIPEDA Principle 4.5 and APP 11.2.

117. PIPEDA does not stipulate precise limits for organizations to retain personal information. Rather, PIPEDA Principle 4.5.2 states that organizations should develop guidelines and implement procedures with respect to the retention of personal information, including minimum and maximum retention periods. In failing to establish maximum retention periods for users' personal information associated with deactivated user accounts, ALM contravened PIPEDA Principle 4.5.2.

Retention of information from inactive profiles

118. Similar considerations apply in relation to accounts that have not been active on the website for an extended period of time.

119. In the case of inactive accounts, while users have not provided an affirmative indication of their intent to no longer use the Ashley Madison services, after an extended period of inactivity it becomes reasonable to infer that the purpose for which the account was opened is no longer

relevant. Therefore, the personal information collected for that purpose should no longer be retained.

120. Consequently, in retaining this personal information beyond its purpose, and in failing to establish maximum retention periods for user information associated with inactive user accounts, ALM has contravened APP 11.2 and PIPEDA Principles 4.5 and 4.5.2.

Retention of information following a full delete

121. It is clear from ALM's Terms and Conditions that a purpose for which it collects information is to process payments. The Terms and Conditions also indicate that ALM will retain and use information to prevent fraudulent chargebacks. The provisions of the Australian Privacy Act and PIPEDA vary with respect to this issue, so we consider the issue separately in relation to each piece of legislation.

Australian Privacy Act

122. Under the Australian Privacy Act, ALM is required to destroy or de-identify personal information once it no longer needs the information for any purpose for which the information may be used or disclosed by it under the APPs. Personal information may be used for the primary purpose of collection. However, it may not be used for a secondary purpose unless certain exceptions apply. The Acting Australian Information Commissioner considers that the primary purpose for which information is collected by ALM is to deliver online dating services. The retention and use of personal information to allow ALM to prevent fraudulent user chargebacks is a secondary purpose.

123. Also under the Australian Privacy Act, an entity can use and disclose information for a secondary purpose where a 'permitted general situation' exists, which includes taking appropriate action in relation to suspected unlawful activity or serious misconduct (see s 16A of the Australian Privacy Act). 'Misconduct' is defined in s 6(1) of the Australian Privacy Act to include 'fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty'. For this exception to apply, the entity must 'reasonably believe' that the collection, use or disclosure of personal information is 'necessary' for the entity to take 'appropriate action'. ALM has satisfactorily explained its business need to retain information to address the risk of fraud.

124. However, to ensure that the use and disclosure, and retention, of user information is limited to what ALM 'reasonably' believes is necessary, ALM must limit the period for which it retains user data to a specified period, that refers to the likelihood of fraud within that time. ALM has provided a reasonable basis for its policy of retaining information for a limited period of time after a full delete. Furthermore, since the incident, ALM has reduced the period that it stores information following a full delete from 12 months to 6 months.

PIPEDA

125. Similarly, under PIPEDA Principle 4.5, personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. PIPEDA Principle 4.5 further specifies that personal information shall be retained only as long as necessary for the fulfilment of the purposes for which it was collected. As mentioned above, while it is clear that a purpose for which it collects this information is to process

payments, Ashley Madison's Terms and Conditions also indicate that the company will retain and use this information to prevent fraudulent charge backs.

126. However, in our view, the fact that photos from deleted accounts were retained in error beyond the period specified by ALM constitutes a contravention of PIPEDA Principle 4.5, as a significant proportion of these photos would have included photos of users. Therefore, the photos would remain personally identifiable, even detached from their respective profiles.

127. However, for the reasons described in the paragraphs above, we are satisfied that ALM's *policy* of retaining user information following a 'full delete' for a limited period of time only to address the problem of user fraud, is permitted under APP 11.2 of the Australian Privacy Act and under PIPEDA Principle 4.5.

Fee for deletion

128. ALM presented an explanation about why certain elements of the full delete option were premium services. Specifically, ALM referred to the full deletion of communications sent to other users. Users of a social network platform would not normally expect that information they had shared with other users would be deleted from those other users' inboxes if they decided to delete their own account.

129. However, the paid full delete option was also the only method available to individuals to have their account profile itself permanently deleted from ALM's databases. Therefore, the fee constitutes a condition for users to exercise their right, under PIPEDA Principle 4.3.8, to withdraw consent for ALM to have their personal information.

130. PIPEDA is silent on whether a fee can be charged for the withdrawal of consent. PIPEDA Principle 4.3.8 indicates that an individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. In this case, the payment of a fee cannot be considered a legal or contractual restriction. This fee was neither communicated nor available to prospective and existing users in the messaging or contractual terms and conditions between ALM and individuals at the critical point of sign up, when individuals were considering, agreeing to, and creating an Ashley Madison account.

131. Therefore, ALM's practice of charging a fee for withdrawal of consent without prior notice and agreement is a contravention of PIPEDA Principle 4.3.8. As previously stated, we note that ALM is not currently charging a fee for the full delete service and we would encourage ALM to continue to not do so.

132. As a general note, we would caution that, even in the event that such contractual agreements were in place prescribing fees for the withdrawal of consent in this case, the reasonableness of such a practice would need to be evaluated in light of such factors as: the adequacy and timeliness of the notice, the actual cost to the organization relative to the fee charged and the likely influence it would have on the individual's right to withdraw their consent.

Recommendations for ALM

133. To address the above findings, and in respect of all of its websites, the OPC and OAIC recommend that by 31 March 2017, ALM:

a) cease its practice of retaining indefinitely personal information of users whose accounts are on deactivated or inactive; determine an appropriate period following account deactivation, or following an extended period of inactivity, upon which to delete personal information, based on ordinary usage patterns and its business needs; inform users of these policies;

b) ensure that it is not holding personal information beyond the retention period described above, and thereafter periodically review its retention policy to ensure that the retention period chosen remains the appropriate period;

c) implement the retention schedule for both future and currently deactivated accounts;

d) implement the retention schedule for both future and currently inactive accounts;

e) commit to continuing to provide a no-cost option for individuals to request the removal of their account profile information (this need not include all of the premium deletion services currently offered as part of the full delete service, such as the deletion of personal information sent to other ALM users from those users' in-boxes); and

f) submit to the OPC and OAIC details of the steps it has taken to comply with the above.

Accuracy of email addresses

Requirement to maintain quality and accuracy of personal information

134. Both the Australian Privacy Act and PIPEDA place an obligation on organizations to take steps to maintain the quality and accuracy of the personal information they collect and use.

135. PIPEDA Principle 4.6 states that personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. Principle 4.6.1 further states that the extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

136. Similarly, APP 10.1 states that APP entities must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete. APP 10.2 imposes the same obligation in relation to personal information that an APP entity will use or disclose, having regard to the purpose of the use or disclosure.

Practices at the time of the data breach

137. After the data breach occurred, searchable databases of email addresses registered on Ashley Madison were published online. A subset of email addresses listed in these databases reportedly belonged to people who had never used Ashley Madison.

138. ALM confirmed that it did not, and does not, verify the email addresses provided by users. In a written submission it submitted:

> *As a matter of policy, ALM did not, and does not, verify the accuracy of any of the personal information of its customers in order to afford users anonymity vis-à-vis other users.*

139. ALM further explained that its decision not to verify email addresses at the time of account sign up was 'the result of a deliberate and considered decision by the company to forgo such verification in order to provide users with anonymity', and that this practice 'enhances privacy and security'. In discussions with the OPC and OAIC, ALM also stated that another reason for not requiring email verification was that it would present a barrier to registration processes, discouraging some individuals from signing up.

140. The email address field is mandatory during account creation on Ashley Madison. Individuals cannot use any of the services of the Ashley Madison website prior to completing this sign up process and providing an email address. However, communication with other users is done through the ALM platform. As such, even if users do not provide their own email address upon sign up, they can still use Ashley Madison services by providing a false email address.

141. In explaining why the email address field was mandatory, ALM stated that it requires users to provide an email address so that it can send website activity notifications, marketing materials and as an authentication measure in the case of a user support request.

142. ALM also sends a 'Welcome' email when a user signs-up. A user cannot opt-out of receiving this welcome email. ALM provides the following information in the footer of the welcome email (and subsequent emails) sent by ALM to enable non-users to correct the situation if their email address is inaccurately associated with an Ashley Madison account:

> Please do not reply to this email message. It was sent from an address that cannot accept incoming email. It won't reach us. For questions or concerns please visit our "Contact Us" page: http: …..
>
> You are receiving this Email Notification because you or someone using your email address has signed up as a member to our service. The email address we have on file for profile number xxxxxxx is [email address]
>
> If you have received this email in error, you wish to delete your account or unsubscribe from Email Notifications, please choose one of the options below:
>
> Unsubscribe from Email Notifications | Delete Account
>
> **USA and Canada Address:**
> PO Box 67027
> Toronto, ON Canada M4P 1E4
>
> **International Address:**
> 9 Karpensiou, 2021 Nicosia

143. While the text of the footer indicates that if the individual has received the message in error they can choose from one of the options below, the two links subsequently presented are only to 'unsubscribe from email notifications' or 'delete account'. The latter option leads to the 'delete profile' page within the user's Ashley Madison account, which prior to the breach required payment for full account deletion.

144. ALM explained that if it is contacted by the real owner of an email address and informed that their email address is being used on one of ALM's websites without permission, ALM will overwrite the inaccurate email address and deactivate the account in question. ALM said that when this occurs, it typically happens after an owner of an email address receives the standard 'welcome email' sent following account creation.

145. ALM indicated that it was aware that some users do not provide their real email addresses when they register on Ashley Madison. ALM would therefore appear to be cognizant of the possibility of harm to non-users, should they receive communications about Ashley Madison in error. In early discussions with the OPC following the breach, ALM indicated that in determining whether or not to issue breach notifications to affected individuals by email, they considered the possible impact on non-users who would receive notifications. ALM ultimately elected to provide direct email notifications to affected users, including Canadian and Australian individuals, but included a prominent statement in those emails, acknowledging that the recipient might not be an Ashley Madison user. The statement read as follows:

> YOU ARE RECEIVING THIS EMAIL FROM AVID DATING LIFE INC. BECAUSE YOUR EMAIL ADDRESS WAS IN OUR DATABASE OF ASHLEYMADISON.COM USERS. IT COULD HAVE

BEEN SUBMITTED BY YOU OR SOMEONE ELSE. WE DO NOT VERIFY EMAIL ADDRESSES PROVIDED TO US THROUGH ASHLEYMADISON.COM, SO THE FACT THAT YOU ARE RECEIVING THIS EMAIL MAY NOT MEAN THAT YOU IN FACT EVER WERE A VISITOR TO OR USER OF ASHLEYMADISON.COM.

Findings

Email as Personal Information

146. As a preliminary issue it is necessary to consider whether email addresses, and the fact of their association with the Ashley Madison website, is personal information.

147. Personal information is defined in PIPEDA as 'information about an identifiable individual', and in the Australian Privacy Act as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'. Common to the two pieces of legislation is that the information in question must be capable of identifying an individual.

148. Some email addresses, even in isolation, clearly identify an individual by name and other identifying information, such as their workplace. For example, the information published online contained an email address that purportedly belonged to the Prime Minister of New Zealand, 'john.key@pm.govt.nz'.[14] However, even where an email address does not identify an individual on its face, it might still identify an individual when combined with other information. For example, it might be possible to conduct an online search to identify the owner of an email address. If that is possible, information associated with the email address is the personal information of that individual.

149. Many of the email addresses associated with the Ashley Madison website, including the examples provided above, would allow an individual to be identified and therefore constitute personal information. Moreover, the apparent association (whether true or not) between the individual and the Ashley Madison website, constitutes personal information.

Sufficient accuracy

150. In representations to the OPC and OAIC, ALM argued that PIPEDA Principle 4.6 and APP 10.1 and 10.2 were designed to protect only users submitting information to organizations, not uninvolved third parties whose personal information may be improperly submitted by a user, and as a result, collected or used by an organization. With respect to PIPEDA, ALM argues that 'the individual' referenced in Principle 4.6.1 only refers, in this case, to the individuals who signed up to ALM, and not to other individuals whose emails addresses were improperly submitted by a user and used without the consent of the true owner of that email address.

151. The Commissioners are of the view that this is not a correct interpretation of either Act. We find no basis, in either provision, to limit an organization's accuracy obligations to personal information about individuals with whom the organization has a direct relationship. As an analogy, by this logic,

[14] 'Ashley Madison leak: Who's been using John Key's name to get lucky?', *New Zealand Herald*, 19 August 2015. This email address was in fact incorrect. The domain 'pm.govt.nz' is not used by the New Zealand government for email addresses.

a lender would have no obligations under the accuracy provisions to consider the impact of identity theft on a victim, as the individual they are dealing with is not the victim (but rather the person impersonating the victim).[15]

152. The Commissioners are of the view that, consistent with the protections afforded elsewhere under the Act, the accuracy provisions are intended to apply to all individuals whose personal information is collected, used or disclosed by an organization, whether or not the individual provided the information to the organization directly.

153. Therefore, as the association between email addresses and the ALM website constitutes personal information, ALM is obliged under PIPEDA and the Australian Privacy Act to address the accuracy of this information.

154. However, neither Act requires that personal information collected, used, and disclosed be absolutely accurate in all cases. Under the APPs, an organization must take steps that are 'reasonable in the circumstances' when collecting, using or disclosing personal information and, for use and disclosures, an assessment of accuracy having regard to the 'purpose of the use or disclosure.' Under PIPEDA, the personal information must be as accurate, complete and up-to-date as is necessary 'for the purposes for which it is to be used.' PIPEDA Principle 4.6.1 specifies that the 'extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual.'

155. At issue is whether the steps taken by ALM to ensure accuracy were reasonable in the circumstances (under the APPs), to ensure email addresses collected and used by ALM were as accurate as necessary for the purposes for which they were to be used, taking into account the interests of the individual (under PIPEDA).

156. In representations to the OPC and OAIC, ALM argued that the chief purpose for the collection and use of email addresses was for ALM to contact users, and submitted that a user who knowingly provides a false email address on sign up is effectively foregoing receipt of such communications. For its part, ALM is prepared to accept that the submission of inaccurate email addresses will impede communications with its users, in what it characterized as the broader interest of enhancing privacy of users. It argued that the email addresses it collects and uses are accordingly as accurate as is necessary. In our view, this assessment that ALM met its accuracy obligations under the APPs and PIPEDA has serious shortcomings for reasons laid out below.

157. In considering whether the steps taken by ALM with respect to the accuracy of email addresses were reasonable under the APPs, it is necessary to have regard to the circumstances in which the information was collected, used and disclosed. This context is similarly important under PIPEDA Principle 4.6, as described in further detail below. In the case of Ashley Madison, the context includes:

    a) the potential for individuals using this type of service to provide false information;

[15] An analogous situation was considered under the Australian Privacy Act in G v TICA Default Tenancy Control Pty Ltd [2004] PrivCmrACD 2 (16 April 2004) in which the Australian Privacy Commissioner considered the steps that the operator of a residential tenancy database was obliged to take to keep the information it held about tenants up-to-date.

b) the particular sensitivity of the nature of the service and any related communications, and the serious implications of a false association with Ashley Madison; and

c) ALM's knowledge that a subset of its users submit false email addresses.

158. In this context the Commissioners are of the view that it was insufficient, in the particular circumstances of the Ashley Madison website, for ALM to assume that since an email address was provided by a user, it must be that individual's email address (rather than that of a non-user).

159. ALM does take some steps to address the issue of non-users' email addresses being inaccurately associated with Ashley Madison. It collects contact information directly from users during account sign up. After this, it sends a welcome email to the email address provided. This welcome email, containing a note in the footer that an individual can contact ALM if the email has been sent to them in error, affords a non-user some opportunity to identify and correct the inaccuracy if their email address has been falsely used by someone else.

160. With respect to this approach, the Commissioners are of the view that the welcome email footer is an insufficient method to address accuracy concerns relating to the email addresses of non-users being inaccurately associated with the Ashley Madison service. This approach places the onus on a non-user to proactively respond to an unsolicited email of unknown origin – a practice which is rightly viewed as a potentially risky activity that individuals should generally avoid.[16]

161. Under PIPEDA Principles 4.6 and 4.6.1 and APP 10.2, ALM's assessment above that the information is sufficiently accurate is not commensurate with the important purpose to which these emails will be put. Specifically, the purpose for which the email addresses are being used is to contact users, not non-users, on a highly personal, sensitive and discreet matter (that is, communications to facilitate discreet affairs). Nor does ALM's approach take into account the interests of the individuals, which includes non-users whose email addresses are used without consent and who may receive an 'unwelcome' communication from ALM that falsely associates them (in their eyes, and the eyes of others) with the company's services.

162. In addition, PIPEDA Principle 4.6.1 also requires that information must be sufficiently accurate to minimize the possibility that inappropriate information may be used to make a decision about the individual. Even absent a data breach, by virtue of ALM sending emails, including, at a minimum, a welcome email, to email addresses provided by users on sign up, ALM is exposing the purported association with Ashley Madison to anyone reading or having access to the email. As a consequence, if emails from the Ashley Madison website were inaccurately sent to a non-user's work or shared home email address, the assumed connection to Ashley Madison could affect

---

[16] See the following guidance for individuals warning against responding to an unsolicited email of unknown origin, and specifically, against clicking 'unsubscribe' links in suspicious emails:
- Australian Communications and Media Authority, *Spam FAQ*, available at <http://www.acma.gov.au/Citizen/Stay-protected/My-online-world/Spam/spam-faqs>;
- Government of Canada, *Protect Yourself Online or While Mobile*, available at <http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00095.html>; and
- Office of the Privacy Commissioner of Canada, *Top 10 tips to protect your inbox, computer and mobile device*, available at <https://www.priv.gc.ca/resource/op-vpel/casl_tips_ind_e.asp>.

decisions made about the individual by an employer, family member, or other acquaintances and cause significant and persistent reputational harm.

163. Given the circumstances identified above and particularly considering the highly unique and sensitive nature of the Ashley Madison website, the Commissioners are of the view that ALM must take further steps to better assure the accuracy of the email addresses that it collects and uses.

164. A range of reasonable options are available to ALM to reduce the inaccuracy of email addresses held by ALM, and the associated risk to non-users being falsely linked to the website. For example, if ALM made the email address field optional, this would largely reduce the incentive and likelihood for users to provide false information, thereby reducing the serious privacy risks to non-users. Making the email address field optional would be in keeping with PIPEDA Principle 4.4 (Limiting Collection). Alternatively, ALM could implement technical measures to reduce inaccuracy, such as an automated process to verify that an email address rightly belongs to the new user.

165. As a final note, ALM submitted that by not verifying email addresses, it is enhancing the privacy of its users by affording them the ability to deny an association with the website. ALM further said that its choice to make the email address field mandatory enhances the privacy of users, arguing that 'if the email field was rendered optional, only those users that wanted to receive email messages to their working address would use the feature,' thus reducing the ability of users who had provided a valid email address to deny their association with the website.

166. The Commissioners do not agree that ALM's practice of making the email address field mandatory, but not verified, is privacy enhancing for users. An approach that creates unnecessary reputational risks in the lives of non-users, in order to provide users with a possibility of denying their association with Ashley Madison, is not in keeping with the intent of either PIPEDA or the Australian Privacy Act. In fact, under the current scheme, a greater relative population of individuals would have the potential reputation impacting cloud of an association with Ashley Madison hanging over them. In such a context, a '*deniable association*' still remains a reputation damaging '*possible association*' in the eyes of decision makers, family members and influencers. The possible benefit to ALM users cannot be considered in isolation without regard to the possible harm to non-users.

167. In conclusion, the Commissioners are of the view that in the particular circumstances of the Ashley Madison website, the steps that ALM takes to assure the accuracy of email addresses associated with new user accounts falls short of what is required by PIPEDA Principle 4.6 and APP 10. By not taking reasonable steps to ensure that email addresses are as accurate as is necessary for the purposes for which they are to be used, and by failing to take into account the interests of the affected individuals (including non-users), ALM has contravened PIPEDA Principle 4.6. Taking these circumstances into account, by not taking reasonable steps to ensure the email addresses it collects are accurate, ALM has contravened APP 10.1., and by not taking steps to ensure the email addresses it uses or discloses are accurate having regard to the purpose for which they are handled, ALM has contravened APP 10.2.

Recommendations for ALM

168. To address the above findings, the OPC and OAIC recommend that by 31 March 2017, ALM:

a) amend its account creation process to allow users to join the Ashley Madison website without providing an email address, or if it continues to require email addresses from new users, implement technical measures to enhance the accuracy of email addresses provided to the reasonable satisfaction of OPC and OAIC; and

b) submit to the OPC and the OAIC details of the steps it has taken to comply with the above.

Transparency with users

Requirement for openness and informed consent

PIPEDA

169. Section 6.1 of PIPEDA states that the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting.

170. PIPEDA Principle 4.8 requires that an organization make information about its personal information handling policies and practices readily available to individuals. Principle 4.8.1 goes on to require that this information shall be made available in a form that is generally understandable.

171. PIPEDA Principle 4.3 states that the knowledge and consent of an individual is required for the collection, use, or disclosure of personal information, except where inappropriate. Principle 4.3.5 notes that in obtaining consent, the reasonable expectations of the individual are also relevant.

172. Finally, Principle 4.3.5 also requires, among other elements, that consent shall not be obtained through deception.

173. Openness and valid consent are important principles to allow individuals to make informed decisions about which organization to entrust with their personal information. Although PIPEDA does not have a general requirement to disclose details about information security to users in order to obtain valid consent, it does require that individuals be able to understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. Accordingly, the investigation considered whether the information ALM provided to users when they were deciding whether to supply ALM with their personal information was adequate.

Australian Privacy Act

174. In the Australian Privacy Act, APP 1 and APP 5 require organizations to inform individual of certain matters concerning the organization's information handling practices. APP 1.3 requires organizations to publish a privacy policy about 'the management of personal information by an entity', and this may include some general information about security measures.[17] However, there is no requirement in the APPs for an organization to explain in detail its security safeguards, or to provide details about its procedure for closing user accounts.

175. As such, the discussion in this section of the report is confined only to ALM's obligations under PIPEDA.

[17] See paragraph 1.20 of the Australian Privacy Principles guidelines.

Practices at the time of the data breach

176. At the time of the data breach, when an individual was deciding whether to sign up as a user on the Ashley Madison website, that decision would have been informed by available sources of information provided by ALM about its personal information handling practices.

177. The first source of information is the Ashley Madison home page. As noted in paragraph 51 above, at the time of the data breach the front page of the Ashley Madison website prominently displayed a series of trust-marks which conveyed a high level of security and discretion for the site. These included a medal icon labelled 'trusted security award', a lock icon indicating the website was 'SSL secure', and a statement that the website offered a '100% discreet service'.

178. The Ashley Madison home page has since been changed by ALM to remove the medal icon labelled 'trusted security award' and the statement that the website offers a '100% discreet service.'

179. The second source of information is ALM's Terms and Conditions and Privacy Policy (accessible via a link from the sign up page). With respect to security safeguards, the Privacy Policy at the time of the data breach said:

> ***Security***
>
> *We treat data as an asset that must be protected against loss and unauthorized access. To safeguard the confidentiality and security of your PII, we use industry standard practices and technologies including but not limited to "firewalls", encrypted transmission via SSL (Secure Socket Layer) and strong data encryption of sensitive personal and/or financial information when it is stored to disk.*

Though not included in the Privacy Policy, the Terms and Conditions said:

> ***I. Privacy & Use of Information***
>
> *You acknowledge that although we strive to maintain the necessary safeguards to protect your personal data, we cannot ensure the security or privacy of information you provide through the Internet and your email messages. Our Privacy Policy is incorporated into the Terms by this reference. You agree to release us, our parent, subsidiaries, and affiliated entities and ours and their shareholders, officers, directors, employees and agents, successors and assigns from all claims, demands, damages, losses, liabilities of every kind, know (sic) and unknown, direct and contingent, disclosed and undisclosed, arising out of or in any way related to the release or use of such information by third parties.*

180. With respect to account closure options and retention, ALM's Privacy Policy states:

> ***How long do you keep the information I've provided you?***
>
> *We keep the information you have given us for at least as long as your Ad Profile stays active or hidden. ….You have the opportunity to opt-out of certain communications and modify personal information or demographic information you have provided to us, and to hide information visible to the public users of the Website at any time by going to the 'Manage profile' or 'message Center' sections on your Ad Profile.*

…Please also note that changing or deleting your information through the 'Manage Profile' or 'Message Centre' section of the system, or opting-out of email notifications from us, will only change or delete the data in our database for the purpose of future activities and communications. These changes and deletions will not change or delete information or emails that are queued to be sent or have already been sent.

181. ALM's Terms and Conditions include the following:

> ***C. Cancellation of Your Account for non-Usage***
>
> *If you have not logged into your account within the previous 90 days, we reserve the right to cancel your remaining credits. ….*
>
> ***F. Termination***
>
> *…You may terminate your access to the Service at any time via our Site or by sending us written or email notice of termination.* ***You will not be entitled to any refund of unused credits or subscription fees upon your termination of your access to our Services for any reason whatsoever.***
>
> ***G. Complete Profile Removal***
>
> *You may also select the "Complete Profile Removal" option, which is offered separately of basic termination. This feature will remove any existence of the account on the Service, including all messages sent and received (regular, collect, priority), Winks, Gifts, all photos you have uploaded, any Site usage history and other personally identifiable information. By using the Service, you hereby acknowledge that Members' communications may no longer be accessible should that Member have selected the Complete Profile Removal.*

182. Only after a user has created a profile on Ashley Madison, would a link be accessible to the user from their profile settings titled 'Delete Profile'. If the user clicked this link, they would be taken to a page explaining, for the first time, that they could completely remove their profile (as described above) for a fee ($19 for Canadian users), or 'hide' their profile for free.

183. As described in paragraph 108 above, after a user chose to pay to delete their profile, and the payment was processed, they would receive a notification indicating:

> *This notice confirms that Ad Profile number … has been successfully deleted from our system. Some information will be retained for 6-12 months due to legal and financial reasons after which it will be removed as well.*

184. The only other reference to the fact that any information would be retained after purchasing a full delete is found separately in the 'Financial Information' section in ALM's Privacy Policy which states that users who provide financial information to ALM '…consent to our providing of your financial information to our service providers and to such third parties as we determine necessary to support and process your activities and transactions, as well as to your credit card issuer for their purposes.'

185. ALM confirmed that in practice all user information, including both financial information and non-financial information, was retained in all cases for 12 months.

186. There are two issues at hand. The first issue is whether the information provided to users as described above was adequate under PIPEDA's Principle 4.8.

187. The second issue is whether the information above, made available to users when they were choosing to provide personal information to ALM, was adequate to ensure that the consent was valid and not obtained through deception.

Findings

188. While ALM did provide some information about their security safeguards and account closure options and retention practices, critical elements of their practices that would have been material to prospective users' decision to join Ashley Madison were either absent, difficult to understand or deceptive. Notably:

    a) While some information on security safeguards was provided in the Privacy Policy and Terms and Conditions, ALM confirmed that the 'trusted security award' trust-mark on their home page was simply their own fabrication rather than a validated designation by any third party.

    b) It is also unclear, even from a careful reading of both the Privacy Policy and Terms and Conditions, that unless a user chooses a full delete, their profile will be retained indefinitely. The wording in the Privacy Policy is that information will be retained 'at least as long as your Ad Profile stays active or hidden.' In another section of the Terms and Conditions it states that if users do not log into their account for 90 days, ALM reserves the right to cancel any remaining credits. This could further confuse the user or lead them to expect that inactivity can alone lead to the deactivation or deletion of their account. In this context, it is not clear that an 'active' ad profile is simply any profile, no matter how old, that has not been hidden or deleted. ALM asserts that the existence of a 'Complete Profile Removal' option separate from 'basic termination' in the Terms and Conditions made it clear that basic termination would not include the deletion of their personal information. We do not agree. This stand-alone description does not counter the impression created by the other statements, and in fact, could serve to further confuse the issue.

    c) Users choosing the full delete option were not informed until <u>after</u> they had paid for the full delete that their information would in fact be retained for an additional 12 months.

189. In this context, ALM did not meet its obligations under PIPEDA Principle 4.8.1 to be open about its policies and practices with respect to the management of personal information, and to make that information available in a form that is generally understandable.

190. In light of the failure to be open about personal information handling practices, it is relevant to consider whether the consent obtained by ALM for the collection of users' personal information was valid, and additionally, whether it was obtained through deception.

191. Section 6.1 of PIPEDA states that consent is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting. Principle 4.3.5 states that in obtaining consent, the reasonable expectations of the individual are also relevant, and that consent shall not be obtained through deception.

192. The particular nature of the Ashley Madison service, including the potential consequences for individuals of unauthorized disclosure of their personal information, makes it reasonable to expect that transparency about information security and retention practices was a critical component of valid consent in this context. Given the nature of the services being offered by the Ashley Madison website (that is, facilitating affairs) and the discretion sought and expected by users, it is reasonable to expect that some individuals might have chosen not to share their personal information with ALM if they had not been misled at registration by the fictitious security trust-mark, and if they had been made aware that ALM would retain their information indefinitely unless they paid a fee for deletion.

193. The fictitious trust-mark appears to have been designed by ALM to deliberately foster a false general impression among prospective users that the organization's information security practices had been reviewed and deemed high quality by an independent third party. This is one of the few pieces of prominently displayed 'information' about ALM's personal information handling practices accessible by prospective users when deciding whether to sign up. Given that this trust-mark goes to the reasonable user's material consideration of security and discretion in these particular circumstances, it is our conclusion that its posting on Ashley Madison's home page invalidated consent, in contravention of PIPEDA Principle 4.3.5.

194. Considered individually and in concert with each other, the OPC is of the view that the lack of clarity regarding retention practices, and the presence of a deceptive trust-mark, could have materially impacted on a prospective user's informed consent to join the Ashley Madison site and allow the collection, use and disclosure of their personal information.

195. Therefore, the failure by ALM to be open about these personal information handling practices is material to the validity of consent. In this context, it is our conclusion that the consent obtained by ALM for the collection of personal information upon user sign up was not valid and therefore contravened PIPEDA section 6.1.

196. In providing false information about its security safeguards, and in failing to provide material information about its retention practices, ALM contravened PIPEDA section 6.1 as well as Principles 4.3 and 4.8.

Recommendations for ALM

197. To address the above findings, the OPC recommends that by 28 February 2017, ALM:

a) review its Terms and Conditions, Privacy Policy, and other information made accessible to users for accuracy and clarity with respect to its information handling practices - this should include, but not be limited to, making it clear in its Terms and Conditions, and on the page on which people choose how to deactivate their accounts, the details of all of the deactivation and deletion options available;

b) review all of its representations, on its website and elsewhere, relating to personal information handling practices to ensure it does not make misleading representations; and

c) submit to the OPC details of the steps it has taken to comply with the above.