Office of the Information and Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Avid Life Media Inc. (the Organization)
Decision number (file number)	P2015-ND-49 (File #001247)
Date notice received by OIPC	July 23, 2015
Date Organization last provided information	August 14, 2015
Date of decision	August 18, 2015
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is based in Ontario. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA and the information was collected from individuals residing in Alberta.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information about the individuals: • height • weight • sex • email address • user name • hashed password The Organization reported that the following additional information is also likely at issue for paid users: • full name • address

	This information is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ☒ unauthorized disclosure
Description of incident	• On July 12, 2015, an employee at the Organization noticed unusual activity on its information systems. • The following day, a threat appeared on customer service representative screens. Hackers threatened to release customer records, as well as employee documents and email communications unless the Organization shut down two of its adult websites, Ashley Madison and Established Men. • On July 19, 2015 the Organization confirmed that hackers had obtained personal information from its servers.
Affected individuals	• Approximately 37 million individuals were affected, including approximately 2.4 million individuals in Canada, 300,000 of which are paid users. • The Organization reported that a number of the affected individuals are residents of Alberta; however, it is still determining how many Albertans were affected.
Steps taken to reduce risk of harm to individuals	The Organization took the following steps: • Shut down websites temporarily. • Engaged cyber security forensics firm. • Set up phone line to respond to enquiries. • Ensured payment processers were aware of incident and taking necessary precautions. • Changed authorization requirements on entire infrastructure. • Rebuilt all computers on network infrastructure. • Interviewed suspected individual and confiscated computer devices. • Notified Toronto Police and the United States Federal Bureau of Investigation; investigations are underway. • Offered free account erase service to all users.
Steps taken to notify individuals of the incident	The Organization reported it is in the process of determining a notification strategy. The Organization reported its concern that notifying affected individuals could increase the likelihood of reputational harm resulting from this incident.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization recognized that, "Given the nature of the sites, secrecy and discretion are of paramount importance to users, and the loss of that secrecy would likely have a significant effect on the personal, and potentially professional, relationships of the customers." In my view, most of the personal information involved is not inherently sensitive. However, the personal information is associated with individual postings on adult websites. In this context, the types of harm that could result from unauthorized access to, and disclosure of, the personal information are hurt and humiliation, and damage to reputation. Individuals may have used the same email addresses and passwords to register on other websites. Email addresses and passwords can be used by unauthorized parties for identity theft and fraud. In my view, these are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported that the likelihood of harm would depend on positive identification and arrest of the suspect and any accomplices, as well as confirmation that all data have been recovered or destroyed. In my view, is likely that the hackers have made and distributed copies of the personal information. I do not agree that the eventual arrest (if any) of the suspect and accomplices would substantively reduce the real risk of harm. In my view, the likelihood of harm resulting from this incident is increased because of the malicious intent and apparent technical ability of the hackers. The hackers have demonstrated malicious intent by issuing a threat. The Organization reported that the individuals' passwords were hashed (scrambled using an encryption algorithm). While this provides a measure of protection, hashed passwords in the hands of a motivated and knowledgeable attacker can be reverse engineered. In my view, there is also a real likelihood of harm resulting from the hackers or other unauthorized recipients of the data reverse engineering the hashed passwords.

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals resulting from this incident. The personal information is associated with postings on adult websites and could be used to cause the harms of hurt and humiliation and damage to reputation. Email addresses and passwords could also be used to cause the harms of identity theft and fraud. These are significant harms. The malicious intent and apparent technical ability of the hackers increases the risk of harm resulting from this incident. I require that the Organization notify the affected Albertans in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the Regulation) and notify me in writing it has done so on or before August 28, 2015, indicating how many individuals were notified. Section 19.1(1)(a) of the Regulation requires that organizations give a notification directly to the individual. Section 19.1(2) authorizes an organization to give a notification indirectly if I determine that direct notification would be unreasonable in the circumstances. If the Organization in this case believes that notifying affected individuals directly will cause significant harm, such as reputational damage, it must provide me with reasons so that I can make a determination as to whether direct notification would be unreasonable in the circumstances.

Jill Clayton
Information and Privacy Commissioner