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	America Online Inc. (Organization)
Decision number (file number)	P2015-ND-77 (File # 000100)
Date notice received by OIPC	May 15, 2014
Date Organization last provided information	May 15, 2014
Date of decision	November 17, 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"	I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • email address, • user name, • contact address, • postal code, • gender, • date of birth, • address book content (work address, spouse, company name, work title, employer, anniversary, etc.), • telephone number, • encrypted and/or hashed password, • encrypted security question.

	Additionally, some information may relate to two (2) employees of the Organization's Canadian subsidiary, including: • employee identification number, • employee contact information, and • employee reviews/endorsements by co-workers and managers of certain skills and attributes. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In April 2014, after noting an increase in the amount of spam appearing as "spoofed emails" from the Organization's mail addresses, the Organization discovered that an intruder had accessed certain of its systems illegally. • The Organization's believes its servers were accessed illegally only in the USA and not Canada, and the intruder acquired user information beginning in August 2013.
Affected individuals	Twenty thousand (20,000) residents of Alberta may have been affected.
Steps taken to reduce risk of harm to individuals	• The Organization investigated the incident. • The Organization changed its Domain-based Message Authentication, Reporting and Conformance (DMARC) policy to notify DMARC-compliant email providers to reject emails from the Organization's email addresses that were not sent from the Organization's servers. • The Organization advised its customers to change their passwords and security questions. • Educational resources on creating strong passwords and spam protection were provided, including tips on how to deal with suspicious emails. • The Organization reported that, prior to the incident, a number of steps were taken to protect personal information including storing personal information in secure data centres, limiting access to information to what is necessary for performing job functions and providing organization-wide privacy and security training.

Steps taken to notify individuals of the incident	Affected individuals were notified via email.
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 did not reference any specific harms that might result from this incident, but noted "the increased incidence of spoofing" that led to its investigation, and steps that were taken to "mitigate against further spam". The Organization also reported "the accessed personal information is not sensitive" and "there is no indication that this incident resulted in disclosure of users' financial information." Finally, the Organization reported that it "has no indication the encryption on the passwords or the answers to security questions was compromised." In my view, the customer personal information involved is sensitive. It contains identity (date of birth) information, email addresses, and additional information in address book content that provides comprehensive individual profiles. This information could be used to cause the harms of identity theft, fraud, and phishing. Also, password hashes could potentially be used to compromise other accounts of individuals who use a single password on multiple sites. These are significant harms. Although the Organization reported that the accessed employee personal information is "not sensitive in the way that traditional performance reviews may be," it did not provide any additional explanation to support this assertion. In previous breach decisions, I have found that this type of personal information can be used to cause the significant harms of hurt and humiliation.
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 "this incident appears to involve wrongful intent," and that it has taken steps to "mitigate against further spam." Overall, it assessed the "risk of harm to the affected individuals is low, such that there is no real risk of significant harm to individuals resulting from this incident." I agree the Organization has reduced the risk of harm somewhat. However, because date of birth was compromised, and considering the number of affected individuals, malicious intent, and the possibility that phishing attacks could occur well after the incident itself, I consider the risk of harm resulting from this incident has not been fully mitigated.

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. The personal information involved sensitive identity information (date of birth), email addresses, and additional information in address book content that provides comprehensive individual profiles. This information could be used to cause the harms of identity theft, fraud, and phishing. Also, password hashes could potentially be used to compromise other accounts of individuals who use a single password on multiple sites. These are significant harms. In the absence of additional information about the employee information, I find this type of personal information can be used to cause the significant harms of hurt and humiliation. Although the Organization took steps to reduce the risk of harm resulting from this incident, considering the number of affected individuals, malicious intent, and the possibility that phishing attacks could occur well after the incident itself, I consider the risks have not been fully mitigated. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner