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	LinkedIn Ireland (Organization)
Decision number (file number)	P2019-ND-154 (File #003233)
Date notice received by OIPC	June 24, 2016
Date Organization last provided information	December 2, 2016
Date of decision	August 26, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • member ID, • email address, and • hashed password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In 2012, the Organization experienced an incident involving unauthorized access to and disclosure of some members' passwords. At the time, the Organization believed that the hashed passwords of 15 million accounts may have been compromised.

	• On May 18, 2016, the Organization became aware of the release of an additional set of data comprised of email addresses, member IDs, and hashed password combinations of more than 100 million members, which appeared to have been obtained from the theft in 2012. • The Organization reports that, at the time of the 2012 breach, other than the hashed passwords that were posted by the intruders at that time, the Organization had no evidence demonstrating that other passwords or personal information had been taken.
Affected individuals	The incident affected more than 100 million members, including 670,000 accounts which identified Alberta in the individuals' profiles.
Steps taken to reduce risk of harm to individuals	• After the 2012 incident, advised users to reset their passwords, reported the incident to law enforcement, and took a number of steps to enhance security, including but not limited to password salting, dual factor authentication, and increased system monitoring. • After the May 2016 discovery, the Organization took a number of actions, including: o invalidated the passwords of users who had subscribed to services before June 6, 2012 and who had not reset their passwords since 2012. o implemented email verification for accounts, a password strength meter and automated monitoring of suspicious account activities. o created an information security team and appointed a Chief Information Security Officer.
Steps taken to notify individuals of the incident	Affected individuals were notified by email between May 26, 2016 and May 29, 2016.
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 specifically identify any harm(s) that might result from this incident, but reported that it "…believes the risk of harm to impacted individuals is low, primarily due to the lack of sensitivity of the affected data". The Organization also said it "…has no complaints or reports that sensitive personal information, such as credit card information, private messaging or job application history, were taken from the site." In my view, a reasonable person would consider that the information at issue (account ID, email address) could be used for phishing and social engineering attacks, increasing individuals' vulnerability to identify theft and fraud and the risk to other online

	accounts. The passwords were not salted and were hashed using SHA-1 hash function that has known security vulnerabilities. These weaknesses make the passwords recoverable from the corresponding hash values thereby putting personal information of individuals whose passwords were not reset following the 2012 incident at risk. Personal information from those individuals' accounts may have been accessed in an unauthorized manner and could be used to commit fraud. 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 it *…believes the risk of harm to impacted individuals is low, primarily due to the lack of sensitivity of the affected data, [the Organization] immediately invalidated the passwords of all …members who had not reset their passwords since June 2012, and since 2012, [the Organization] has no complaints or reports that sensitive personal information, such as credit card information, private messaging or job application history, were taken from the site.* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the breach resulted from malicious intent (deliberate intrusion, theft), a significant number of accounts were compromised, the personal information was disclosed on the dark net, and the password hash values were vulnerable to compromise as the passwords were not salted and their hash values produced using SHA-1, which has known security vulnerabilities.

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.

A reasonable person would consider that the information at issue (account ID, email address) could be used for phishing and social engineering attacks, increasing individuals' vulnerability to identify theft and fraud and the risk to other online accounts. The passwords were not salted and were hashed using SHA-1 hash function that has known security vulnerabilities. These weaknesses make the passwords recoverable from the corresponding hash values thereby putting personal information of individuals whose passwords were not reset following the 2012 incident at risk. Personal information from those individuals' accounts may have been accessed in an unauthorized manner and could be used to commit fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the breach resulted from malicious intent (deliberate intrusion, theft), a significant number of accounts were compromised, the personal information was disclosed on the dark net, and the password hash values were vulnerable to compromise as the passwords were not salted and their hash values produced using SHA-1, which has known security vulnerabilities.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand affected individuals were notified by email between May 26, 2016 and May 29, 2016 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner