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	Snap-on Incorporated (Organization)
Decision number (file number)	P2018-ND-074 (File #008901)
Date notice received by OIPC	June 7, 2018
Date Organization last provided information	June 7, 2018
Date of decision	July 6, 2018
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 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: • full name, • email address, and • salted and hashed password. This information is about identifiable individuals (registered users) and is "personal information" as defined in section 1(1)(k) of PIPA. The information was in a database accessible through one of the Organization's public online stores, buy1.snapon.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In early April, a third-party security provider alerted the Organization to suspicious activity involving potential unauthorized access to customer information.

	• The Organization investigated and determined that between March 25 - 26, 2018 an unauthorized third-party accessed and acquired the full names, email addresses, and salted and hashed passwords of certain registered users within a database accessible through one of the Organization's public online stores, buy1.snapon.com. • Other personal information in the database was encrypted and there is no evidence that this data was accessed or acquired. Payment card numbers would not have been accessible because the Organization uses a third party to handle payment processing, and does not receive any payment card information; therefore, the information was not present in the database.
Affected individuals	The Organization reported that there are approximately 4,290 users registered for the province of Alberta that could have been affected by this incident.
Steps taken to reduce risk of harm to individuals	• Initiated an internal investigation, notified law enforcement and engaged a cybersecurity forensic firm. • Took immediate steps to remediate the issue and eliminate the unauthorized access. • Disabled the website. • All users will be required to establish a new user name and password when the new website is relaunched.
Steps taken to notify individuals of the incident	The Organization reported that it would notify registered users in Alberta by mail sent the week of June 6, 2018.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 harms that might result from this incident but advised affected individuals that they "…should exercise caution when responding to any unsolicited emails requesting your personal information or account credentials, or emails that link you to a website that requests you to enter personal information or account credentials." Further, "If you receive such an email purporting to be from [the Organization], please do not enter your personal information or your account credentials." In my view, the information at issue could be used to send unsolicited emails and for phishing. I have previously said that phishing is a significant harm.

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 did not specifically assess the likelihood of harm resulting from this breach but, as noted above, advised potentially affected individuals to "exercise caution when responding to any unsolicited emails" and said "We also encourage you to follow best practices and routinely change your passwords (especially in cases where you used the password on our site with other accounts)". In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion), the information has not been recovered, and considering the number of potentially affected individuals in Alberta alone.

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 as a result of this incident.

The information at issue could be used to send unsolicited emails and for phishing. I have previously said that phishing is a significant harm. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion), the information has not been recovered, and considering the number of potentially affected individuals in Alberta alone.

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

The Organization reported that it would notify registered users in Alberta by mail sent the week of June 6, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner