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	Calgary Co-operative Association Limited (Organization)
Decision number (file number)	P2018-ND-161 (File #008273)
Date notice received by OIPC	April 12, 2018
Date Organization last provided information	November 26, 2018
Date of decision	December 3, 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 whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(l) 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 all or some of the following information: • name, • address, • telephone number, • email address, • last 4 digits and expiry date of credit card used for purchase, and • total cost of purchase. This information is about identifiable individuals and is "personal information" as defined in section 1(1) (k) of PIPA. The information was collected via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On March 28, 2018, a customer of the Organization received an anti-virus alert notifying him of an attempt to download malicious software to his computer when he visited the Organization's website. The customer notified the Organization. • The Organization investigated and, on April 3, 2018, discovered unauthorized modification of the website "shop.coopwinespiritsbeer.com", which was formerly "www.yycwinedeals.com" and still redirected from that URL. • The Organization said the only authorized administrators of the site are its IT team and the vendor and neither undertook any changes. The Organization believes it is possible that unmitigated vulnerabilities in WordPress were exploited in order to gain administrative privileges. • The Organization reported that unauthorized individuals had access to, but did not necessarily read, the data.
Affected individuals	The incident affected 670 individuals.
Steps taken to reduce risk of harm to individuals	Permanently took down website.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 11, 2018.
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 reported that "no harm" might result from this incident. In my view, a reasonable person would consider that the contact, financial and profile information at issue (total amount spent, relationship to the Organization, last four digits/expiry of credit card), as well as email address, could be used for unsolicited telephone calls, emails and phishing, as well as increased risk of fraud. These are all 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 harm is "not significant" and there are "no personally identifying information types (sic)"… and the likelihood that harm could result is "low". In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and modification). The Organization acted quickly to notify affected individuals, which will likely help to prevent and detect some types of harm; however, this cannot entirely mitigate the risk that significant harm will result from this incident.

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 contact, financial and profile information at issue (total amount spent, relationship to the Organization, last four digits/expiry of credit card), as well as email address, could be used for unsolicited telephone calls, emails and phishing, as well as increased risk of fraud. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and modification). The Organization acted quickly to notify affected individuals, which will likely help to prevent and detect some types of harm; however, this cannot entirely mitigate the risk that significant harm will result from this incident. I require the Organization to notify the affected individuals whose information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals in an email on April 11, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner