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	Bunzl North America (Organization)
Decision number (file number)	P2021-ND-094 (File #013384)
Date notice received by OIPC	June 10, 2019
Date Organization last provided information	June 10, 2019
Date of decision	March 30, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals whose personal information was collected in Alberta, 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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following: • Individual #1: Full name, telephone number, address, billing email address, credit card number and expiry (NOTE: this card expired in 2013) • Individual #2: Full name, telephone number, partial address (NOTE: address is a box number only and does not appear to exist), billing email address, credit card number and expiry This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization also said it "does not have enough information to definitively say that the information associated with these accounts is business contact information". "Business contact information" is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information."

	Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the information at issue was not collected, used or disclosed "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." As a result, the business contact information is not excluded from the application of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• Western Safety Products (WSP) is a division of the Organization and is a Seattle, Washington based distributor of safety equipment to businesses. • WSP had a web-based e-commerce site which was hosted by a third party. The website was closed in February 2018; however, unauthorized parties appear to have gained access and re-activated the site on September 19, 2018. It appears the administrative portal used by the third party hosting the site was compromised, and as a result, order information may have been exposed to an unauthorized third party. • The breach was discovered on April 1, 2019 when a customer contacted the Organization with concerns about a compromised credit card (the concerns were not related but an investigation found the compromised site).
Affected individuals	The incident affected 2 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Shut down the third party e-commerce web site. • Disabled the web service on the virtual server hosted by the third party. • Retained an independent IT forensics firm to investigate. • Moved email services on the third party virtual server to MS 365 and set up multi-factor authentication.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on June 10, 2019.

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 "Card compromise is possible (though this is unlikely in the case of Individual #1 as the card information is outdated). The possible disclosure of the billing email address could lead to phishing attempts." In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and 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 "WSP believes the likelihood of harm is small, in light of the expired or incomplete/ incorrect information available." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious intent (deliberate action by an unauthorized party). The information was exposed for over 6 months before the compromised was discovered.

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 and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious intent (deliberate action by an unauthorized party). The information was exposed for over 6 months before the compromised was discovered.

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 the affected individuals were notified by letter on June 10, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner