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	Herff Jones LLC (Organization)
Decision number (file number)	P2022-ND-001 (File #022059)
Date notice received by OIPC	July 1, 2021
Date Organization last provided information	July 1, 2021
Date of decision	February 11, 2022
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's head office is in Indianapolis, Indiana, USA. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue may have included: • first and last name, • address, • telephone number, • email address, • payment card information, and • limited order-related information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information at issue was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On April 7, 2021, the Organization became aware of suspicious activity involving certain customers' payment card information.

	• In late May, the Organization determined that certain customer personal information was subject to unauthorized access. • The Organization reported that forensic evidence shows activity related to unauthorized access to and exfiltration of payment card information occurred during the period of January 11 to April 19, 2021.
Affected individuals	The incident affected 63 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Launched an investigation, notified law enforcement, and engaged a cybersecurity firm to assist in assessing the scope of the incident. • Took steps to mitigate the potential impact to its customers. • Took steps to further protect its systems and data, including changing administrative passwords, implementing more restrictive firewall rules, and deploying industry leading web application firewalls. • Offered customers a free hotline for any questions concerning this incident. • Secured an identity monitoring service at no cost to customers for one year. • Decommissioned proprietary payment processing system. • Encouraged customers to monitor their payment card account statements and credit reports for instances of unauthorized activity and report any suspicious or unusual activity to their financial institution.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter and email starting July 1, 2021.
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, "The possible harms associated with the compromise of payment card information include fraud." 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 the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and 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, *The likelihood of harm is minimized by our offer of one year of free credit monitoring to all potentially impacted individuals, to help ensure that any unathorized [sic] activity is quickly identified and reported to financial institutions.* In my view, a reasonable person would consider 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). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed were to be used for fraudulent purposes. The information may have been exposed for approximately three (3) months.

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 the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and 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). Although the Organization has put additional safeguards in place, these were not in place at the time of the breach. Further, this does not necessarily mitigate the potential harm that may result if the information accessed were to be used for fraudulent purposes. The information may have been exposed for approximately three (3) months.

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 by letter and email starting on July 1, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner