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	Savers, Inc. (Organization)
Decision number (file number)	P2021-ND-123 (File #017855)
Date notice received by OIPC	October 23, 2020
Date Organization last provided information	April 6, 2021
Date of decision	April 27, 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 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)(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 all or some of the following information: • name, and • bank account number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 28, 2020, the Organization was the victim of a phishing attack that targeted one employee and the information contained in their email account. • The incident was discovered on July 3, 2020 when the Organization noticed the employee's email account was being used to send fraudulent emails, attempting to initiate a fraudulent money transfer.

Affected individuals	The incident affected 147 individuals, including 2 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Secured the employee's email account. • Investigated the incident with the assistance of a cybersecurity firm. • Encouraged individuals to monitor their account statements for unauthorized activity. • Implemented additional safeguards and technical security measures to protect personal information. • Providing additional training to employees.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on October 22, 2020.
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 reports: *It appears that the goal of the attack was to perpetrate fraud against [the Organization] rather than to collect personal information of ... employees or other individuals. However, it is possible that this personal information could be used for financial fraud against the two Alberta residents. To date, no such fraud has been reported to [the Organization].* I accept the Organization's assessment that a reasonable person would consider the financial information at issue could be used to cause the significant harm of financial fraud.
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 reports: *It appears that the goal of the attack was to perpetrate fraud against [the Organization] rather than to collect personal information of ... employees or other individuals. No fraud or other misuse of personal information has been reported to [the Organization] to date. At this point, [the Organization] considers it unlikely that harm will result to the two Alberta residents.* 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 a third party (phishing, attempted fraudulent money transfer). The lack of reported fraud or misuse to date does not mitigate against future harms, as fraud and identity theft can occur months or years after a breach.

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 the financial information at issue could be used to cause the significant harm of financial fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (phishing, attempted fraudulent money transfer). The lack of reported fraud or misuse to date does not mitigate against future harms, as fraud and identity theft can occur months or years after a breach. 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 Organization notified affected individuals in a letter dated October 22, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner