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	Harry Rosen Inc. (Organization)
Decision number (file number)	P2023-ND-003 (File #028042)
Date notice received by OIPC	November 15, 2022
Date Organization last provided information	December 19, 2022
Date of decision	February 1, 2023
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 a national fashion retailer based in Ontario. 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: <u>Clients</u> • name, email address, loyalty tier, last transaction date, and customer ID. <u>Group A Employees</u> • name, hire date, date of birth, mailing addresses, bank account number, dependent name and date of birth, customer number for benefits provider, benefits coverage, social insurance number, customer number for pension plan, contribution amounts to pension plan, employee number, and compensation information. <u>Group B Employees</u> • Subgroup one: name, customer number for pension plan, and contribution amounts to pension plan • Subgroup two: name, employee number, and compensation 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 was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Threat actor(s) accessed the Organization's network without authorization and used this access to deploy ransomware that encrypted files and likely also to steal data. • The Organization is continuing to monitor the dark web. • The Organization's forensic investigation is continuing.
Affected individuals	The incident affected 160,000 individuals, which includes 16,000 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the breach to the Toronto Police Service. • Notified its benefits provider. • Offered credit monitoring to all current employees (irrespective of exposure). • Implemented additional security safeguards.
Steps taken to notify individuals of the incident	Affected clients were notified by email on November 10, 2022. Affected current employees were notified by email on October 14, 2022. The Organization reported that affected former employees' notification is forthcoming.
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, *For clients, there is a risk of phishing.* *For Class A Employees, there is a risk of identify fraud.* In my view, a reasonable person would consider that contact and email addresses, particularly in conjunction with brand affiliation and identification could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Contact, identity and employee information could be used for the purposes of the significant harms of identity theft and fraud, financial loss, embarrassment, hurt or humiliation, and damage to reputation or relationships. Beneficiary, spouse, or dependent information, especially with respect to children or other vulnerable groups,

	could be used to cause harms of embarrassment, hurt or humiliation. All of the above 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, *Harry Rosen acknowledges that the risk to affected Clients and Class A Employees is real and non-speculative.* I agree with the Organization's assessment. In my view, a reasonable person would consider that 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.

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.

Contact and email addresses, particularly in conjunction with brand affiliation and identification could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Contact, identity and employee information could be used for the purposes of the significant harms of identity theft and fraud, financial loss, embarrassment, hurt or humiliation, and damage to reputation or relationships. Beneficiary, spouse, or dependent information, especially with respect to children or other vulnerable groups, could be used to cause harms of embarrassment, hurt or humiliation. All of the above are 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.

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 current employees and affected client by email on October 14, 2022 and November 10, 2022 respectively and in accordance with the Regulations. I understand that affected former employees have not been notified to date.

The Organization is required to notify the affected former employees in Alberta and is required to confirm to my Office, within ten (10) days of the date of this decision, that affected former employees have been notified of this incident in accordance with the requirements outlined in section 19.1 of the Regulation.

Cara Stelmack
Assistant Commissioner, Operations and Compliance