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	Holt, Renfrew & Co. Ltd. (Organization)
Decision number (file number)	P2020-ND-131 (File #016492)
Date notice received by OIPC	July 20, 2020
Date Organization last provided information	August 24, 2020
Date of decision	November 6, 2020
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 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 a combination of all or some of the following information: • names, • date of birth, • Social Insurance Number • driver's license number, • passport number, • credit card number, • debit card number, • termination letter, • offer letter, • salary increase notification letter, • signature, • direct deposit information (copy of voided cheque or direct deposit form with branch and account information), • benefits (summary of benefits package), • medical information (doctor's note with diagnosis, a receipt for a medical test), • financial information (messages about personal banking matters), and

	• T4 information not related to the Organization. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that personal information was collected in Alberta, this Office has jurisdiction in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On April 9, 2020, the Organization's IT department was notified about a phishing attack and potential password compromise. • The Organization discovered that on April 8, 2020, a phishing email was sent to six employees from a legitimate email account associated with one of the Organization's concession partners. • The phishing email was designed to prompt email recipients to click a link to download several documents. The link in the email took users to a Microsoft OneNote page that prompted users to click another link to download the documents securely. This second link took users to a fake Microsoft Office 365 login page that was designed to harvest the user's credentials. • The investigation found that the threat actor successfully obtained two employees' email credentials through this phishing attempt. The threat actor made use of those credentials on April 8 and 9, 2020, and interacted with the employees' mailboxes, including creating inbox rules to evade detection.
Affected individuals	The incident affected approximately 19,780 individuals including 2,202 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Manually reviewed the data file containing extracted personal information elements (the file contained approximately 25,000 lines). • Alerted its concession partner whose email address was associated with the phishing email. • Alerted those who received further a phishing email that it was not a legitimate email and to delete it. • Blocked accounts and the passwords, and changed passwords. • Employed a variety of sterilization measures on the affected computers. • Implemented multi-factor authentication for the affected email accounts.

	• Adopted a new email security cloud solution to add multiple email security measures, in addition to the existing filtering. • Refreshing its anti-phishing training for all employees. • Notified the Toronto Police, the Canadian Anti-Fraud Centre, and the Canadian Centre for Cyber-Security about the incident. • Notified the Privacy Commissioner of Canada and intended to notify the Commission d'accès à l'information (Quebec) and the Information and Privacy Commissioner of British Columbia on or before July 20, 2020. • Auditing all employees' email accounts with a view to ensuring that confidential and personal information is either deleted or archived to a secure drive in compliance with its current Retention Policy. • Investigating options to technologically contain the size of email accounts or the degree to which they contain historical information (e.g., automatically archiving messages to a secure drive). • Revising its Record Retention policy in light of the above new measures. • Arranged free credit monitoring and identity theft product for 10 years for those individuals whose Social Insurance Number, driver's license number, passport number, credit/debit or other account number may have been compromised.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail, email and telephone on August 20, 2020. The Organization is currently re-sending notification those whose notification was ineffective the first time.
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: *Identity theft and financial fraud are possible harms. Embarassment (sic) is also possible (in the case of spending and related information). Discrimination is possible (in case of holidays, which are indicative of religious beliefs).* In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms.
Real Risk The likelihood that the significant harm will result must	The Organization reported:

be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	*We have determined that there is a real risk of harm -- given both the nature of some of the information that was compromised (e.g., identification numbers) and the fact that the threat actor is an unknown party. However, to date, Holt Renfrew is not aware of any harms having arisen.* 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 (phishing attack) and it appears the personal information may have been used to send emails, with the purpose of obtaining information for fraudulent purposes. The Organization reported that it was not aware of any harms having arisen; but this is not a mitigating factor, as identity theft and fraud can occur months and even years after a data 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.

In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. These are all significant harms. 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 (phishing attack) and it appears the personal information may have been used to send emails, with the purpose of obtaining information for fraudulent purposes. The Organization reported that it was not aware of any harms having arisen; but this is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email, mail, and telephone on August 20, 2020, and is re-sending notification to those whose notification was ineffective the first time. The Organization is not required to notify affected individuals again.

Elaine LeBuke
Senior Information and Privacy Manager