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	CPT Group, Inc. (Organization)
Decision number (file number)	P2019-ND-020 (File #008526)
Date notice received by OIPC	April 30, 2018
Date Organization last provided information	December 7, 2018
Date of decision	February 14, 2019
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 information: • name, • address, and • social insurance number. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected by the Organization via email. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 22, 2018, the Organization began investigating after phishing emails were sent from an employee email account. • The Organization determined that an unknown individual had access to an employee's email account from November 22, 2017 to December 8, 2018.

	• The Organization reported that it does not know if any sensitive personal information was accessed without permission.
Affected individuals	The incident affected one individual residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated with assistance from a computer forensics firm. • Enhanced its existing network and email security, including implementing multi-factor authentication. • Re-educating staff and training its employees to help prevent a similar incident. • Notified affected individuals and offered complimentary credit monitoring services, call center services. • Notified regulatory agencies.
Steps taken to notify individuals of the incident	The affected individual was notified in writing on April 27, 2018.
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 "The risk for financial loss is minimized because [the Organization] is notifying the potentially affected individuals and is offering complimentary one-year membership and identity theft protection services. The Organization provided a telephone number for potentially affected individuals to call with any questions they may have." In my view, a reasonable person would consider that the contact and identity information at issue could be used to cause the significant harms of identity theft and 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 did not specifically assess the likelihood of harm resulting from this incident but reported that "On April 27, 2018, (the Organization) began mailing written notifications to potentially affected class members". The Organization also noted that it "…is offering complimentary one-year membership and identity theft protection services. The Organization provided a telephone number for potentially affected individual to call with any questions they may have." 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). The unauthorized party had access for up to 18 days. The Organization reported it does not know if any sensitive personal information was accessed without permission. There is no way to confirm the unauthorized party did not access or copy the information in some form.

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 individual. A reasonable person would consider that the contact and identity information at issue could be used to cause the significant harms of identity theft and fraud. 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). The unauthorized party had access for up to 18 days. The Organization reported it does not know if any sensitive personal information was accessed without permission. There is no way to confirm the unauthorized party did not access or copy the information in some form. I require the Organization to notify the affected individual 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 the affected individual in writing on April 27, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner