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	Cassels Brock & Blackwell LLP (Organization)
Decision number (file number)	P2018-ND-162 (File #009835)
Date notice received by OIPC	September 21, 2018
Date Organization last provided information	November 19, 2018
Date of decision	December 3, 2018
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 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, • email address, • telephone number, • credit card information, • banking information, • invoices, and • description of legal work. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 21, 2018, an unidentified party gained access to the email account of an employee of the Organization.

	• Between August 21 and August 22 the unidentified party sent phishing emails to third parties, and likely ex-filtrated the contents of the employee's email account. • The Organization discovered the breach on August 22, 2018, when clients who had received the phishing email started to question if it was legitimate. • The Organization said the suspected cause of the incident is a phishing email containing a malicious link that was received by the employee.
Affected individuals	The incident affected 197 individuals, 11 of whom reside in Alberta.
Steps taken to reduce risk of harm to individuals	• Disabled the affected email account and email access from outside the Organization's VPN, scanned the employee's computer and confirmed that no malware or other malicious code was present. • Investigated the employee's computer and created a new user account and password for the employee. • Notified third parties who received the phishing email from the employee's email account and told them not to open the phishing email or its attachments, and warned them of the potential their credentials may have been compromised. • Verified that no other staff members received or opened the phishing email. • Retained a third party digital forensic firm to investigate and confirm containment of the incident, assist in analyzing and processing the items in the affected email account, and search the Dark Web to determine if any of the data was posted. • Changed passwords for the Organization's employees in the financial department. • Continuing to investigate whether other individuals may be affected. • Offering complimentary credit and identity theft monitoring for one year to all individuals whose credit cards or banking information was affected.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter between September 21, 2018 and November 14, 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	The Organization reported "…for individuals whose credit card or banking information was affected, there is a potential risk of fraud. For others, there is a potential risk of phishing." I agree with the Organization's assessment. The contact and financial information at issue (credit card and banking information) could be used to cause the harms of identity theft or fraud. The

non-trivial consequences or effects.	contact information, as well as email address, could be used for unsolicited telephone calls, emails and phishing, leading to an increased risk of fraud. These 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 that "Based on the information that is presently known… the harm could be significant because the Incident involved an unknown party maliciously gaining access to the employee's email account. It is possible that the unknown person may use the personal information in the account to cause harm to affected individuals." The Organization also said "It is likely that the attacker may use the personal information to harm affected individuals… it is likely that the unauthorized individual exfiltrated the contents of the email account and has access to the emails and attachments." I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action of an unknown third party (deliberate action) and phishing emails were sent. Further, the Organization reported it is likely the personal information was ex-filtrated, and as such, cannot be recovered.

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.

The contact and financial information at issue (credit card and banking information) could be used to cause the harms of identity theft or fraud. The contact information, as well as email address, could be used for unsolicited telephone calls, emails and phishing, leading to an increased risk of fraud. These are significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to malicious action of an unknown third party (deliberate action) and phishing emails were sent. Further, the Organization reported it is likely the personal information was ex-filtrated, and as such, cannot be recovered.

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 September 21, 2018 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner