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	Eastern Virginia Medical School (Organization)
Decision number (file number)	P2020-ND-147 (File #0015828)
Date notice received by OIPC	May 13, 2020
Date Organization last provided information	May 13, 2020
Date of decision	November 17, 2020
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 a medical school in Norfolk, Virginia, USA, and is an "organization" as defined in section 1(1)(i) of PIPA. The Organization is not a health custodian as defined in Alberta's *Health Information Act* (HIA), such that the HIA would apply in this matter.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • business email address, • social security number, and • wage information of current and former employees. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that some of the email addresses may qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e mail address, business fax number and other similar business information."

	Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized disclosure of the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 28, 2020, the Organization became aware of suspicious activity associated with one of its email accounts. • The Organization's investigation determined that an unauthorized user had gained access to four email accounts for a limited period of time. • The email accounts may have contained emails and documents containing employees' personal information.
Affected individuals	The incident affected one (1) Alberta resident.
Steps taken to reduce risk of harm to individuals	• Advised affected individuals to remain watchful of their email accounts. • Changed passwords associated with the affected email accounts. • Continuing to evaluate additional controls that can be implemented. • Provided additional training to its employees on how to recognize and respond to malicious emails.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by letter sent on May 13, 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	The Organization reported it "…is unaware of any misuse of the information at issue. However, the possible harms that may occur, if the information is misused, includes identity theft and phishing." In my view, a reasonable person would consider that the contact, identity and employment information at issue could be used to

important, meaningful, and with non-trivial consequences or effects.	cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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: *There is no objective evidence that the unauthorized user is in possession of any information pertaining to any of the affected individuals. [The Organization] is unaware of any misuse of the information at issue. It is unlikely that harm would result from this incident, however [the Organization] has notified the affected individuals in any event so that they may protect them-selves.* 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 (deliberate intrusion into an employee's email account). The Organization said it was unaware of any misuse of the information; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for an unknown period of time.

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 that the contact, identity and employment information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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 (deliberate intrusion into an employee's email account). The Organization said it was unaware of any misuse of the information; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for an unknown period of time.

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

I understand the Organization notified the affected individual by letter sent on May 13, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner