Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization	Ernst & Young LLP (Organization)
Decision number (file number)	P2024-ND-001 (File #030965)
Information received by OIPC	On June 30, 2023, the Organization, through legal counsel, informed my office about the unauthorized access of personal information under the Organization's control. My office contacted the Organization's legal counsel in July and September 2023. On September 15, 2023, the Organization, through legal counsel, stated "*there is no real risk of significant harm to individuals as a result of the incident.*" My office followed-up with legal counsel in October and November 2023, requesting clarification on whether the Organization is notifying the Commissioner under section 34.1 of the *Personal Information Protection Act* (PIPA). My office received no responses.
Date Organization last provided information	September 15, 2023
Date of decision	January 15, 2024
Summary of decision	Section 34.1(1) of PIPA states "An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure." Pursuant to section 37.1 (1) of PIPA, "Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure ... " Based on information provided by the Organization on June 30,

	August 3, and September 15, 2023, I have determined that a reasonable person would consider that there exists a real risk of significant harm to individuals as a result of the unauthorized access to personal information in this case. As such, I require the Organization 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 professional services firm. The Organization meets the definition of "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, • address, • email address, • "other contact information," • date of birth, • gender, • marital status, • "certain financial information," • insurance information, • health card, • "certain other personal health information," • employee personal information, including ○ compensation, benefits, and • government-issued identification numbers. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization obtains secure data transfer services (*MOVEit*) from its third-party service provider *Progress Software Corp*. • On May 31, 2023, the Organization learned that its third-party vendor discovered a critical vulnerability in the *MOVEit* application by way of a public notice issued by the third-party. • On June 3, 2023, the Organization's investigation determined the Organization was affected by the vulnerability and that

	personal information "had potentially been exfiltrated on May 27, 2023 by malicious actors." • On June 5, 2023, the Organization confirmed personal information had been exfiltrated by a threat actor. • According to the Organization, on June 6, 2023, the threat actor publicly issued threats to publish data it had exfiltrated from impacted organizations. • On June 22, 2023, the threat actor named the Organization as having been impacted in the attack. • On or about July 7, 2023, the threat actor published "certain [Organization] data files." • On September 15, 2023, the Organization, through legal counsel, confirmed data exfiltrated by the threat actor was "made … available online."
Affected individuals	The incident affected 2,474 residents of Alberta.
Steps taken to reduce risk of harm to individuals	The Organization offered credit monitoring and identity theft protection services to certain affected individuals.
Steps taken to notify individuals of the incident	713 individuals "in the Province of Alberta" were notified in writing between July 26 and September 12, 2023. On September 15, 2023, the Organization's legal counsel advised an additional 1,761 individuals were to be notified in the Province of Alberta within "four weeks" (by or about October 13, 2023). The Organization's legal counsel did not respond to October 24 and November 16, 2023, requests from my office to confirm whether notification to all affected individuals had been completed.
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.	On September 15, 2023, the Organization's legal counsel stated: *[T]here may be an increased risk of phishing to impacted individuals. Additionally, individuals whose sensitive personal information was impacted are at an increased risk of identity theft or fraud.* I agree with the Organization's assessment. A reasonable person would consider that the contact, identity, financial, insurance, employment, and personal health information at issue could be used to cause the harms of financial loss, identity theft and fraud. Personal health information could be used to cause the harm of embarrassment. Email addresses could be used for the purposes of phishing, increasing affected individuals' vulnerability to identity theft and fraud. These are all significant harms.
Real Risk The likelihood that the	On September 15, 2023, the Organization's legal counsel stated:

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.	*To [the Organization's] knowledge, there has not been any evidence of further misuse of the posted data.* *[The Organization] is not aware of any actual harm to potentially affected individuals. [The Organization's] view is that there is no real risk of significant harm to individuals as a result of the incident.* 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 a threat actor, including deliberate intrusion, exfiltration of personal information, and publication of exfiltrated personal information. The lack of evidence or awareness that the personal information has been "further" misused is not a mitigating factor as identity theft, fraud, financial loss, and embarrassment can occur months or years after a data breach. The threshold is "real risk of significant harm," not a lack of awareness of any "further misuse" as submitted by the Organization.

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, identity, financial, insurance, employment, and personal health information at issue could be used to cause the harms of financial loss, identity theft and fraud. Personal health information could be used to cause the harm of embarrassment. Email addresses could be used for the purposes of phishing, increasing 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 a threat actor, including deliberate intrusion, exfiltration of personal information, and publication of exfiltrated personal information.

The lack of evidence or awareness that the personal information has been "further" misused is not a mitigating factor as identity theft, fraud, financial loss, and embarrassment can occur months or years after a data breach. The threshold is "real risk of significant harm," not a lack of awareness of any "further misuse" as submitted by the Organization.

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 713 individuals in writing between July 26 and September 12, 2023 in accordance with section 19.1 of the Regulation. The Organization is not required to notify these individuals again.

On September 15, 2023, the Organization, through legal counsel, indicated its intent to notify the remaining 1,761 affected individuals by or about October 13, 2023. However, despite requests from my office, the Organization failed to confirm it had directly notified the remaining affected individuals in accordance with section 19.1 of the Regulation.

The Organization is required to confirm to my office, within fourteen (14) days of the date of this decision, that the Organization has notified affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, and to provide my office with a copy of the notification.

Cara-Lynn Stelmack
Assistant Commissioner, Case Management