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	Novotech Technologies Corporation (Organization)
Decision number (file number)	P2022-ND-064 (File #023678)
Date notice received by OIPC	October 20, 2021
Date Organization last provided information	February 16, 2022
Date of decision	November 18, 2022
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 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 located in Ottawa, Ontario. It 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:
	• credit application data,
	• bank account number,
	• current and past employee T4's and T5's, which includes:
	  ○ name,
	  ○ address,
	  ○ compensation information,
	  ○ social insurance number,
	• "Electronic funds transmission and automated clearinghouse transmission files for payroll", which includes:
	  ○ name,
	  ○ salary,
	  ○ banking information,
	• "AP and customer direct withdrawals", which includes:
	  ○ name,
	  ○ invoice amount,
	  ○ banking information, and
	• benefit applications for current employees, which includes:
	  ○ name, and

	○ "general health questions from a registration form". This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent that the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 21, 2021, the Organization discovered it experienced an unauthorized access when the Ottawa Police alerted them to a "suspected data leak". • On September 27, 2021, the Organization found that exfiltrated records were publicly disclosed on the dark web. • An investigation determined that "one of [the Organization's] corporate data drives was improperly accessed and certain information was exfiltrated." • The Organization believes a third party remote access appliance – which was susceptible to a known vulnerability – may have been exploited "roughly 6 months prior to the reporting" of the incident (approximately April 2021).
Affected individuals	The incident affected 53 individuals, including 2 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged legal counsel, worked with law enforcement, and conducted an investigation into the breach. • Obtained information from the Canadian Centre for Cyber Security. • Notified other Canadian Privacy Commissioners' offices. • Removed the compromised network appliance. • "Fortifying … IT infrastructure". • Offered affected individuals identity theft and credit monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on October 20, 2021.
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 the possible harm of fraudulent misuse. In my view, a reasonable person would consider that the identity (name, address, social insurance number) and financial (credit application, banking, compensation) information could be used to cause the harms of fraud or identity theft. Information in credit and benefit applications could be used to cause the harms of

non-trivial consequences or effects.	embarrassment, hurt or humiliation. 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: *The likelihood that the harm identified above will result is moderate. At this stage, [the Organization] does not have direct evidence that the personal information has been misused as a result of the unauthorized access. Nonetheless, the personal information involved was sensitive and and [sic] there is a possibility of misuse by threat actors.* The Organization's notification letter read, in part: *On September 27th the data was published on the dark web.* 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 (deliberate intrusion, exfiltration and publication of records). The threat actor potentially had access to the Organization's network as early as April 2021 until the breach was contained in September 2021. Further, records were published on the dark web.

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 identity (name, address, social insurance number) and financial (credit application, banking, compensation) information could be used to cause the harms of fraud or identity theft. Information in credit and benefit applications could be used to cause the harms of embarrassment, hurt or humiliation. These are 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 (deliberate intrusion, exfiltration and publication of records). The threat actor potentially had access to the Organization's network as early as April 2021 until the breach was contained in September 2021. Further, records were published on the dark web.

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 by letter on October 20, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance