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	Petrowest Corporation, Petrowest GP Ltd., Petrowest Civil Services LP, Petrowest Construction LP, Petrowest Transportation LP, Petrowest Services Rentals LP, Petrowest Environmental Services LP, Trans Carrier Ltd. and CJM Trucking Ltd. (the "Organizations") The Organizations are in receivership. Ernst and Young Inc. (the Receiver) reported the breach pursuant to section 34.1 of PIPA.
Decision number (file number)	P2019-ND-046 (File #008274)
Date notice received by OIPC	April 12, 2018
Date Organization last provided information	July 20, 2018
Date of decision	March 7, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organizations are required to notify 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 Organizations are "organization[s]" 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: <u>Employee information</u> • name, • address, • date of birth, • work history (hire and termination dates), • salary, • bank deposit information, • employment history (discipline/awards), • Social Insurance Number, • tax information, • health-related information used for managing benefits, • drug testing information, and • WCB reports.

	<u>Customer-related personal information</u> • name, • contact information, and • the fact that a payment was made (but not the details). 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 in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On or about February 22, 2018, the Organizations noted their systems had been infected with ransomware essentially making them unavailable/inaccessible. • Malicious actors had access to the Organizations' IT systems and data for about eight hours. • All systems were backed up but the backup servers were also infected and there were no current off line backups. • The mail server was not infected. However, the Organizations' mail database was hosted on a file server which was infected, so by the time the hacker got to the mail server, he or she had already disabled its ability to send email. • The Receiver has been and remains unable to access the Organizations' IT systems or data, other than paper records and records kept on third party systems.
Affected individuals	• The incident affected approximately 1,000 to 1,500 individuals from British Columbia and Alberta. • At the time of the appointment of the Receiver, the Organizations had 406 employees.
Steps taken to reduce risk of harm to individuals	• Shut down all externally available terminal servers and assessed the damage. • Determined that all online servers and desktops had been affected, including backup servers. • Disinfected active viruses from all servers and spun terminal servers back up without network access to determine attack and timeline details. • Reported the situation to the Receiver. • Removed the remote desktop application installed by the attacker on the mail server.

Steps taken to notify individuals of the incident	• The Receiver notified 406 employees on April 17, 2018 by email and/or mail. • Historic employees were not notified.
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 Receiver reported "Employee information…was, however, in the systems during the time the hackers had access. This information might be useful to a malicious criminal for identity theft purposes. Notification of the Incident may benefit the data subjects' ability to protect themselves from this risk, however small". In my view, a reasonable person would consider that the contact (name, address), identity (date of birth, SIN), and employment information (salary, T4, banking information) could be used to cause the significant harms of identity theft, fraud and financial loss. The health-related information (benefits information, drug testing results and WCB reports) could be used to cause the significant harms of hurt, humiliation and embarrassment.
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 Receiver reported: *Given the incident was perpetrated by a malicious attacker, [the Receiver] is cognizant that this dictates a heightened suspicion of enhanced risk to data potentially exposed during the Incident. However, some other details of the hacking Incident …may indicate that the target was the mail servers which attackers were attempting to enlist to be captive spambots. The IT specialists consider that the target was not the relatively small number of employees, but rather the servers' functionality as spam bots.* *The breach was contained, lasting 8 hours on February 21-22, 2018. The systems have been taken offline, and as an artifact of the Incident, remain encrypted.* *The unauthorized hackers have not been specifically identified. There is no reason to suspect that the attack was targeted to [the Organization's] employees. No credit card or payment information was exposed.* In my view, a reasonable person would consider 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 and installation of ransomware). Further, the information at issue may have been

	exposed for approximately eight hours, and remains inaccessible, and the Organizations cannot rule out that the information was exfiltrated.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Receiver 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 (name, address), identity (date of birth, SIN), and employment information (salary, T4, banking information) could be used to cause the significant harms of identity theft, fraud and financial loss. The health-related information (benefits information, drug testing results and WCB reports) could be used to cause the significant harms of hurt, humiliation and embarrassment. 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 and installation of ransomware). Further, the information at issue may have been exposed for approximately eight hours, and remains inaccessible, and the Organizations cannot rule out that the information was exfiltrated.

I require the Organizations 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 Receiver notified 406 individuals in an email and/or letter on April 17, 2018 in accordance with the Regulation. The Organizations are not required to notify these individuals again; however, I understand historic employees have not been notified

With respect to notifying affected historic employees, the Receiver reported that "based on its perception and reasonable belief that data was destroyed and not exfiltrated, constrained financial and human resources, and time required to compile useful contact information and identities of data subjects involved in the face of destruction of available records and backups, there are no current plans or readily available resources to attempt to identify other ex-employees to whom notification might be made…should credible evidence of exfiltration of information during the incident comes to light, and it becomes reasonable to expect exfiltration caused an increase in risk to the legitimate interests of ex-employees, then (the Receiver) remains prepared to revisit the decisions it has made with respect to further notification."

Section 19.1(1) of the Regulation states "Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must …be given directly to the individual". However, pursuant to section 19.1 (2), "…where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

The Receiver has explained why it may not be reasonable to directly notify the historic employees of this breach. However, the Receiver has not explained how these individuals are distinguished from the 406 individuals in terms of the likelihood that they will experience significant harm.

Pursuant to section 37.1(2) of PIPA which states "… the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate…".

I require the Organizations (the Receiver) to report to my office in writing, within ten (10) days of the date of this decision, how the likelihood of significant harm resulting to the historic employees is distinguished from the same risk to the 406 individuals that were already notified. The Organizations should also consider and propose means for notifying historic employees indirectly.

Jill Clayton
Information and Privacy Commissioner