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	ExecuPharm, Inc. (Organization)
Decision number (file number)	P2020-ND-071 (File # 015696)
Date notice received by OIPC	April 17, 2020
Date Organization last provided information	April 17, 2020
Date of decision	July 16, 2020
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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information may be at issue for Alberta employees affected by this incident: • name, • address, • email address, • telephone number, • Social Insurance Number, • bank account number, and • physician/nursing licence number. For one employee, a passport number may also have been involved. The name and date of birth of the designated beneficiaries of two of the five Alberta employees may have been involved. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization is a United-States-based entity that provides staffing solutions for parent company, Parexel International Corporation ("Parexel"). • On March 13, 2020, the Organization became aware that its data network had been compromised as a result of a cyber ransomware event conducted by malicious actors. The malicious actors encrypted files and sought a ransom in exchange for lifting the encryption. The Organization was able to successfully rebuild its systems from backup servers without paying the ransom. • The Organization also reported that its "…employees worldwide (including employees based in Alberta) received phishing emails from the malicious actors… [who] may have accessed and/or shared select personal information relating to [Organization] personnel, as well as personal information relating to select personnel of Parexel, whose information was stored on the [Organization's] data network".
Affected individuals	The Organization reported the incident affected 5 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Assembled a crisis management team to coordinate investigation, containment, remediation and restoration. • Launched a forensic investigation. • Engaged external cybersecurity experts and legal counsel. • Reported to the Organization's insurer and U.S. law enforcement. • Developed an informational microsite to update impacted individuals, as well as share support options and resources. • Worked with forensic consultants to rebuild the impacted servers from back up servers and fully restored and secured the Organization's systems. • Implemented additional countermeasures to block phishing and other potentially malicious emails. • Upgraded security measures to prevent future attacks. • Offered a credit monitoring solution to affected individuals in Alberta.
Steps taken to notify individuals of the incident	Affected individuals in Alberta were notified by letter on April 15, 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 important, meaningful, and with non-trivial consequences or effects.	The Organization reported "The impacted employee personal information, if in fact accessed, could potentially allow the malicious actors to commit identity theft". The Organization also said "With respect to the impacted beneficiaries, given the limited and non-sensitive nature of the personal information impacted for those individuals, the Company maintains that there is no real risk of significant harm to the impacted beneficiaries". In my view, a reasonable person would consider the contact, identity (including beneficiary date of birth), and financial information potentially at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud.
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 said it was reporting the breach … > *… in an abundance of caution based on circumstantial evidence (specifically, the malicious actors did encrypt certain Company servers, appear to have exfiltrated information (what was exfiltrated is unknown), and have stated that they accessed employee information). As far as the Company is aware, no damage has been sustained by any of the current or former Company employees in Alberta to date.* The Organization also said that "to date, there is no conclusive evidence that the malicious actors actually accessed such personal information or, if they did, that the malicious actors still have personal information in their possession. However, the malicious actors are claiming they have this information and have threatened to release employee personal information on the dark web". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because it resulted from the malicious action of an unknown third party, who made a ransom demand. Although the Organization was able to rebuild its system and did not pay a ransom, it nonetheless cannot confirm that the malicious actors who compromised the system did not exfiltrate personal information that could be used to cause significant harm. The lack of reported damage or harm to potentially affected individuals to date does not mitigate against the possibility of such harm occurring in the future.

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 the contact, identity (including beneficiary date of birth), and financial information potentially at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because it resulted from the malicious action of an unknown third party, who made a ransom demand. Although the Organization was able to rebuild its system and did not pay a ransom, it nonetheless cannot confirm that the malicious actors who compromised the system did not exfiltrate personal information that could be used to cause significant harm. The lack of reported damage or harm to potentially affected individuals to date does not mitigate against the possibility of such harm occurring in the future. 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 affected individuals in Alberta were notified by letter on April 15, 2020; however, I am not sure if this includes beneficiaries or not (as the Organization assessed there to be no real risk of significant harm to beneficiaries). **The Organization is required to confirm to my office in writing, within 10 days of the date of this decision, that all affected individuals have been notified in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner