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	Parvus Therapeutics Inc. (Organization)
Decision number (file number)	P2020-ND-032 (File #014085)
Date notice received by OIPC	December 3, 2019
Date Organization last provided information	February 14, 2020
Date of decision	March 6, 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 incident involved all or some of the following information: Census-related information of two Albertans: • name, • position, • date of hire, • reporting relationship, • gender, and • salary. Employment Agreement for one Albertan: • name, • position, • date of hire, • date of birth, • address, • social insurance number, • compensation information, • job duties, and • signature.

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On November 19, 2019, a consultant who provides human resource services to the Organization was targeted with a phishing email from an unauthorized account. • The email requested the consultant provide certain human resource information about employees of the Organization. • The consultant did not identify the email as a phishing request and, on November 20, 2019, and responded to it, disclosing the personal information at issue. The breach was discovered the same day. • The Organization is not aware of any breach of or incursion into any of its security systems.
Affected individuals	The incident affected 3 Albertans.
Steps taken to reduce risk of harm to individuals	• Conducted an investigation to confirm the scope of and remediate the incident. Engaged information technology consultants to undertake a root cause analysis of the incident and provide advice, as well as external legal counsel. • Notified the service provider for the unauthorized account to file a fraud complaint. • Advised all employees to change their passwords. • Offered free credit monitoring services to the one Alberta employee whose employment agreement was disclosed. • Notified privacy authorities in applicable jurisdictions about the incident. • Will provide training and instruction to employees about the dangers associated with phishing and cybersecurity incidents. • Will review security systems to increase the effectiveness of spam filters and consider further administrative, physical or electronic safeguards to lessen the risk of such an incident in the future.
Steps taken to notify individuals of the incident	All affected individuals were notified of the phishing incident by email on November 21, 2019. The one Alberta employee whose employment agreement was disclosed was provided with follow-up verbal notification of the disclosure on November 27, 2019.

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 that "The primary harms that could result from this incident are those related to humiliation, reputational damage and embarrassment. It is also possible that the one Alberta employee whose employment agreement was disclosed could be at risk of the harms of fraud, financial loss and identity theft in these circumstances." I agree with the Organization's assessment. A reasonable person would consider that the contact and employment information at issue could be used to cause the harms of hurt, humiliation, embarrassment and reputational damage. Particularly when associated with identity information (such as date of birth, social insurance number), the information could be used to cause the harms of identity theft and fraud. 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 that it is… *… of the view that there is a low likelihood that harm will result from the incident in these circumstances. There are different circumstances that influence the analysis in this respect.* *On the one hand, the personal information at issue was accessed through a targeted phishing attempt by an unknown third party and the one Alberta employee whose employment agreement was disclosed contained information about his engagement by a university in Spain, including his Spanish social security number.* *On the other hand, much of the personal information that was mistakenly disclosed is not particularly sensitive and the affected individuals have already received notice of the incident. Additionally, [the Organization] has arranged for credit monitoring services to be available to the one Alberta employee whose employment agreement was disclosed to lessen the likelihood that harm will result from the disclosure of his personal information.* 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 action). Personal information that could be used to cause significant harms was disclosed.

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 and employment information at issue could be used to cause the harms of hurt, humiliation, embarrassment and reputational damage. Particularly when associated with identity information (such as date of birth, social insurance number), the information could be used to cause the harms of identity theft and fraud. 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 an unknown third party (deliberate intrusion). Personal information that could be used to cause significant harms was disclosed. 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 email on November 21, 2019, and provided follow-up verbal notification to one Albertan on November 27, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner