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	Envision Pharma Group Ltd. (Organization)
Decision number (file number)	P2022-ND-031 (File #022548)
Date notice received by OIPC	May 25, 2021
Date Organization last provided information	May 25, 2021
Date of decision	May 2, 2022
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 service provider in the medical affairs and healthcare communications industry. 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: • name, • postal code, and • social insurance number. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On or about January 26, 2021, the Organization experienced a ransomware incident. • An unauthorized third party gained remote access to certain of its internal computer networks. • The Organization determined that the unauthorized third party acquired some non-public data from its networks. • The Organization reported that the earliest known date of unauthorized third-party activity was on January 19, 2021. There has been no observed malicious activity since January 26, 2021.
Affected individuals	The Organization reported the incident affected 1 individual whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated the incident with the support of outside cybersecurity experts. • Reported the incident to law enforcement. • Worked with outside experts to determine whether personal information was involved. • Determined the incident did not involve a separate client-hosting environment. The vast majority of its clients' data is housed in this separate environment. • Performed multiple external vulnerability scans. • Deployed additional endpoint security monitoring technologies to ensure all systems were brought back online safely. • Performed a dark web search and engaged in monitoring. Neither action has found compromised Envision data. • Regularly evaluates its security protocols and procedures. • Offered 24 months of free identity theft and credit monitoring services.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on May 25, 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 non-trivial consequences or effects.	In its privacy breach incident notification to my office, the Organization did not provide an assessment of the harm that may occur as a result of this incident. However, its notification to the affected individual stated: *We encourage you to contact Equifax and take advantage of the credit monitoring and identity theft protection services we are providing to you free of charge. Remain vigilant and carefully review your accounts for any suspicious activity... If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or*

	company with which the account is maintained...If you would like to take additional steps to protect your personal information, attached to this letter are helpful resources on how to do so. In my view, a reasonable person would consider the contact and identity information at issue could be used to cause the significant harms of 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 reported, *Envision is not aware of any cases of identity theft, fraud, or financial losses to customers stemming from this incident and does not believe the unauthorized third party was targeting personal information in the incident.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised by the malicious action of an unknown third party (deliberate intrusion, ransomware incident). The lack of reported incidents resulting from this breach to date is not a mitigating factor. Identity theft and fraud can occur months and even years after a data breach. Although the Organization reported that it "does not believe the unauthorized third party was targeting personal information in the incident," I do not find this to be reassuring. The Organization can only speculate as to the motives of the unknown third party.

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 individual.

A reasonable person would consider the contact and identity information at issue could be used to cause the significant harms of identity theft and fraud.

The likelihood of harm resulting from this incident is increased because the personal information was compromised by the malicious action of an unknown third party (deliberate intrusion, ransomware incident). The lack of reported incidents resulting from this breach to date is not a mitigating factor. Identity theft and fraud can occur months and even years after a data breach. Although the Organization reported that it "does not believe the unauthorized third party was targeting personal information in the incident," I do not find this to be reassuring. The Organization can only speculate as to the motives of the unknown third party.

I require the Organization to notify the affected individual 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 the affected individual by letter on May 25, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance