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	The HIDI Group Inc. (Organization)
Decision number (file number)	P2022-ND-071 (File #023159)
Date notice received by OIPC	September 2, 2021
Date Organization last provided information	September 2, 2021
Date of decision	January 9, 2023
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 operates in Alberta and 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, • address, • banking information, • SIN, • passport number, • health benefits information. This information is about identifiable individuals 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 August 10, 2021, the Organization had a cybersecurity incident, which may have resulted in staff's personal information being accessed. • The Organization's team of third party cyber security experts

	could not confirm if data access or exfiltration occurred. • In addition, throughout the investigation, the third party investigation found no evidence of misuse or publication of any employee personal information.
Affected individuals	The incident affected fifteen (15) individuals.
Steps taken to reduce risk of harm to individuals	• Took steps to block the unauthorized access and secure confidential information. • Engaged a team of cyber security experts to contain and investigate the incident. • Offered credit monitoring for 12 months. • Added additional security to system. • Engaged external experts to conduct regular security assessments.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on August 30, 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.	The Organization reported the possible harms that may occur as a result of the breach is a "*risk of identity theft or fraud*." In my view, a reasonable person would consider the contact, identity and banking information could be used to cause identity theft, financial loss or fraud. Health benefit information could be used to cause hurt, humiliation or embarrassment. 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 will result was "unknown". In the notice to affected individuals, the Organization reported, "*We want to stress that we are not aware of any misuse of this information...*and*... It is important to note that there is no evidence confirming that the personal information of all current and former employees has been misused 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. The Organization reported that there was no evidence confirming that personal information has been misused; however, the lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach.

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. Contact, identity and banking information could be used to cause identity theft, financial loss or fraud. Health benefit information could be used to cause hurt, humiliation or embarrassment. 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. The Organization reported that there was no evidence confirming that personal information has been misused; however, the lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident. Identity theft can happen months and even years after a data breach. 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 August 30, 2021, in accordance with the Regulations. The Organization is not required to notify the affected individuals again.	

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance