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	Dynamic Insight Corp. (Organization)
Decision number (file number)	P2022-ND-014 (File #022001)
Date notice received by OIPC	June 30, 2021
Date Organization last provided information	January 19, 2022
Date of decision	April 1, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the 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 Organization reported the incident involved some or all of the following information: • name, • date of birth, • phone number, • email address, • address, • social insurance number (SIN), • provincial health number, • certain medical information, and/or • bank account number. 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 March 1, 2021, the Organization learned that an unauthorized individual accessed an employee email account.

	• Certain email contacts of the employee received phishing emails thereafter. • The account may have been accessed as a result of a phishing email. • The Organization reported that no claim files were affected.
Affected individuals	The incident affected approximately 985 individuals, 833 of whom involved information collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Secured the affected account and commenced an investigation with the assistance of outside cybersecurity experts. • Forced a password reset for all accounts. • Implemented multifactor authentication on all accounts. • Demoted privileges for certain accounts. • Offered credit monitoring and an identity theft product for two years at no cost. • Informed affected individuals on other ways to protect themselves from fraud.
Steps taken to notify individuals of the incident	Affected individuals were notified by email from June 28, 2021 to July 2021. Additional notifications were sent after July 15 for cases in which email notifications were undeliverable or email address were unknown. All notifications were completed by October 14, 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, *Dynamic Insight has offered the individuals a premiere credit monitoring and identity theft protection product free of charge to reduce the risk of harm and to mitigate potential harm. Dynamic Insight also provided additional information about steps that the individuals can take to further protect themselves.* In my view, a reasonable person would consider that the contact, identity, medical, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation or embarrassment. These are all 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, *Dynamic Insight considers the risk of harm to the individuals from this incident to be low based on the unauthorized individual's apparent motivation to send phishing emails rather than collect personal information and the lack of evidence of misuse of any of the 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 intrusion into an employee's email account). Although the Organization reported that "*the unauthorized individual's apparent motivation to send phishing emails rather than collect personal information and the lack of evidence of misuse of any of the information*", I do not find this to be reassuring. The Organization can only speculated as to the motives of the thief.

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, identity, medical, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation or embarrassment. These are all 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 into an employee's email account). Although the Organization reported that "the unauthorized individual's apparent motivation to send phishing emails rather than collect personal information and the lack of evidence of misuse of any of the information", I do not find this to be reassuring. The Organization can only speculated as to the motives of the thief.

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 completed notification of affected individuals by October 14, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Information and Privacy Commissioner