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	GroupHEALTH Family of Companies (Organization)
Decision number (file number)	P2021-ND-060 (File #015706)
Date notice received by OIPC	April 27, 2020
Date Organization last provided information	June 1, 2020
Date of decision	March 9, 2021
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 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: <u>Employees and Former Employees</u> • first name, • last name, • banking/electronic funds transfer information (including bank account number), • date of birth, • home address, • home telephone, • cell phone, • Social Insurance Number, • driver's license number, • gender, • place of birth, and • last addresses. <u>Job Applicants</u> • first name, • last name, • home address, • home telephone number,

	• cell phone number, • personal email address, • employment and educational history, and • reference name and contact information. <u>Plan Members</u> • first name, • last name, and • limited information relating to a subset of claims (including drug identification number). <u>Applicants for certain company products/services</u> • first name, • last name, • telephone number, • address, and • credit card expiry/type (but not card number or CVV). <u>Non-employee EFT recipients</u> • first name, • last name, • banking/electronic funds transfer information, including bank account number. <u>Other non-employee individuals</u> • first name, • last name, • Social Insurance Number, • home address, and • personal email address. 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 or around March 26, 2020, an employee of the Organization was notified by a third party about a suspicious email sent from the employee's email account. • The employee reported the suspicious activity to the Organization's IT department.

	• The Organization and a third party cybersecurity firm investigated the incident. • The Organization believes that: (a) the employee's email account was accessed by an unauthorized third party; (b) the period of potential unauthorized access to the employee's email account is approximately March 17, 2020 to March 25, 2020; and (c) unauthorized access was limited to the employee's email account and did not affect other accounts.
Affected individuals	The incident affected approximately 698 individuals, including approximately 75 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Offered all employees two years of free credit monitoring and identity theft protection services. • Extended the same offer to other affected individuals as appropriate based on the nature of the information that was in the employee's email account as reasonably assessed. • Reported the incident to law enforcement. • Performed searches of the dark web in an effort to identify activity in relation to the affected information. • Notified data protection authorities.
Steps taken to notify individuals of the incident	Current employees were notified of the incident by email on April 20, 2020, with a follow-up on April 30, 2020. Other affected individuals were notified of the incident by email or letter on April 30, 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 risks of harm to individuals as a result of this incident include the following:* • *identity theft, financial loss and fraud;* • *negative effects on a credit record;* • *hurt or humiliation in connection with certain claims and benefits information; and* • *email phishing or spear-phishing attacks.* I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud, and have a negative effect on the individual's credit record. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses could be used for

	the purposes of phishing, increasing vulnerability to identity theft and fraud. 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 did not specifically assess the likelihood that significant harm would result from this incident, but informed affected individuals in the breach notification that it was "offering you two years of free credit monitoring and identity theft protection services…" and outlined additional steps affected individuals could take to protect themselves. 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). Further, the information may have been exposed for approximately 9 days.

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 and financial information at issue could be used to cause the harms of identity theft and fraud, and have a negative effect on the individual's credit record. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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). Further, the information may have been exposed for approximately 9 days.

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 the affected individuals by email on April 20, 2020 and by email and letter on April 30, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner