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	Wilson M. Beck Insurance (Alberta) Inc. (Organization)
Decision number (file number)	P2021-ND-213 (File #020128)
Date notice received by OIPC	March 10, 2021
Date Organization last provided information	April 28, 2021
Date of decision	November 1, 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 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, • address, • date of birth, and • credit card information. 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 February 2, 2021, a phishing email was sent to an employee of the Organization. • The breach was discovered on February 2, 2021 when an employee emailed the Organization's IT department after a client reached out regarding a suspicious email received from the employee.

Affected individuals	The incident affected 578 individuals.
Steps taken to reduce risk of harm to individuals	• Locked down the affected user and performed a password reset. • Reviewed the inbox rules for the affected user. • Cleaned up inbox rules and autoreply configurations.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on March 10, 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: *Identity theft is potential harm arising from (sic) breach. Only if those emailed actioned the instructions within the email would there be the potential for further harm.* Further: *Identity theft could result in a scarred credit history, denials of loans and mortgages, or not being able to open a bank account because of your scarred credit history.* In my view, 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. 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: *Identity theft could result in a scarred credit history, denials of loans and mortgages, or not being able to open a bank account because of your scarred credit history.* Further, its notice to affected individuals, said… *...if you have forwarded private information …via (employee name) such as credit card numbers and/or other private financial information we ask that you contact your Credit Card Company and your Financial Institution to advise them of the potential threat. We further recommend that you contact the credit reporting agencies and set up a credit watch to ensure your financial safety.* 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). The Organization confirmed that there was an unauthorized access to personal information. Additionally, the information may have been exposed for approximately 7 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. 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 into an employee's email account). The Organization confirmed that there was an unauthorized access to personal information. Additionally, the information may have been exposed for approximately 7 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 March 10, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner