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	CareVest Capital Inc. (Organization)
Decision number (file number)	P2023-ND-012 (File #027827)
Date notice received by OIPC	October 25, 2022
Date Organization last provided information	October 25, 2022
Date of decision	February 17, 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 is headquartered in Calgary, 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, • date of birth, • mailing address, • telephone number, • email address, • financial account number, • Social Insurance Number, and • cheque images. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On April 20, 2022, an employee was victim to a phishing attack. • The incident was discovered on April 28, 2022. • The Organization believes the attack resulted in the compromise of an email inbox.
Affected individuals	The incident affected 4,619 of individuals, including 3,016 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Isolated the affected employee's account(s) and forced a password reset. • Provided credit monitoring services to affected individuals. • Notified the Canada Revenue Agency. • Providing employee training on cybersecurity and online safety. • Implemented additional technical safeguards.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on October 7, 2022.
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: *Since the information impacted is mostly financial in nature there is a risk of identity theft. There is also a risk of cheque fraud as images of voided cheques were found in the compromised inbox.* I accept the Organization's assessment. A reasonable person would consider that the identity (name, date of birth, Social Insurance Number), contact (email/mailing address, telephone number) financial (account number, cheque image) information at issue could be used to cause the harms of identity theft, fraud, financial loss, and negative affects on a credit record. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to 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 "acknowledges that the risk facing affected individuals is real and non-speculative." I agree with the Organization's assessment. 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 unauthorized actors (phishing, deliberate intrusion). The unauthorized actor(s) had access to the employee's email account for approximately 8 days prior to discovery of the incident.

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. The identity (name, date of birth, Social Insurance Number), contact (email/mailing address, telephone number) financial (account number, cheque image) information at issue could be used to cause the harms of identity theft, fraud, financial loss, and negative affects on a credit record. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to 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 unauthorized actors (phishing, deliberate intrusion). The unauthorized actor(s) had access to the employee's email account for approximately 8 days prior to discovery of the incident. 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 October 7, 2022, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance