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	InvestX Financial (Canada) Ltd. (Organization)
Decision number (file number)	P2022-ND-34 (File #023959)
Date notice received by OIPC	November 9, 2021
Date Organization last provided information	November 9, 2021
Date of decision	May 13, 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 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 located in Vancouver, British Columbia, 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, • email address, • mailing address, • telephone number, • social insurance number, • "general investor information", • investment details, and • bank or brokerage account information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that they do "not have office in Alberta, but in certain cases information may have been collected by brokers in Alberta." To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On September 24, 2021, the Organization was victim to a ransomware attack. • An investigation determined that a threat actor obtained system administrator credentials and exploited "corporate firewalls to access Amazon AWS hosting infrastructures." • The Organization did not rule out the possibility that personal information was exfiltrated.
Affected individuals	The incident affected 284 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Offered identity theft monitoring services to affected individuals. • Notified law enforcement. • Implemented a cybersecurity awareness program. • Reviewed safeguards and enhanced certain security capabilities. • Conducted penetration testing of hosting and office infrastructure.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail or email, beginning on November 9, 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 that "fraud and identity theft are the main risks of harm as a result of the breach." I accept the Organization's assessment. A reasonable person would consider that contact (name, address, email, telephone), identity (social insurance number) and financial (investment, banking/brokerage account) information at issue could be used to cause the harms of identity theft, fraud, and possibly financial loss or negative effects on a credit record. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to the above. 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: *[There] is no evidence, at this time, that any of the information involved was misused or that any individual has suffered from identity theft or financial fraud as a result of the breach. However, because of the sensitivity of the information that was potentially accessed by the threat actors, [the Organization] believes that this incident creates a real risk of significant harm to individuals.*

	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 the malicious action of a threat actor (deliberate intrusion, deployment of ransomware, possible exfiltration of personal information). A lack of evidence that personal information was misused does not mitigate against future harm. Identity theft, fraud, and phishing can occur months or years after a 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.

A reasonable person would consider that contact (name, address, email, telephone), identity (social insurance number) and financial (investment, banking/brokerage account) information at issue could be used to cause the harms of identity theft, fraud, and possibly financial loss or negative effects on a credit record. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to the above. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due the malicious action of a threat actor (deliberate intrusion, deployment of ransomware, possible exfiltration of personal information). A lack of evidence that personal information was misused does not mitigate against future harm. Identity theft, fraud, and phishing can occur months or years after a 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 mail or email beginning on November 9, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance