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	Mawer Investment Management Ltd. (Organization)
Decision number (file number)	P2021-ND-334 (File #022382)
Date notice received by OIPC	July 20, 2021
Date Organization last provided information	August 12, 2021
Date of decision	March 10, 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 Calgary, AB 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, • telephone number, • email address, • mailing address, • account number, • financial institution account numbers, • social insurance number, and • company (employment) information. 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 July 9, 2021, an unauthorized actor circumvented multi-factor authentication safeguards and gained access to an employee email account. • An investigation determined that the unauthorized access lasted approximately one hour; during the incident, the unauthorized actor conducted searches about financial transactions, browsed email messages, and may have exfiltrated a mailing list.
Affected individuals	The incident affected 5,404 individuals, including 2,830 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Reset all passwords. • Invalidated tokens for all users. • Disabled additional credentials for the compromised user. • Notified financial institutions. • Notified law enforcement. • Offered credit monitoring services to some affected individuals. • Implemented a number of changes to administrative and technical safeguards, including disabling some legacy IT services.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and telephone on July 16, 2021. Additional affected individuals were notified by email on August 3, 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: *The incident is associated with a risk of phishing communications targeted at affected clients and arisk [sic] of third-party identity-related fraud* I agree with the Organization's assessment. A reasonable person would consider that the contact, identity (social insurance number), 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 or spear-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 did not provide a clear assessment of risk of harm to affected individuals. However, they reported: *… the unauthorized person:* *-Had access to its e-mail system for slightly over an hour* *-Conducted some searches that suggest an interest in finding communications about our pending financial transactions.* *-Browsed a set of e-mails, and* *-Discovered —and spent the most time on—a mailing list the company had used to invite individuals to a firm event that was attached to one of the e-mails* In an update dated August 12, 2021, The Organization said: *The entire content of the compromised e-mail account was unlikely to have been taken by the unauthorized person.* *Some e-mail messages containing personal information in the account were likely browsed by the unauthrozied [sic] person.* ***There is circumstantial evidence that suggests the mailing list (which includes enough information to enable targeted phishing) was taken by the unauthrozied [sic] person.*** *[emphasis added]* The notice to affected individuals read: *We do not know who the unauthorized person is or whether they could attempt to use information to impersonate you or someone from [the Organization], so we ask you to be on guard.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown actor who deliberately circumvented safeguards to access emails and may have exfiltrated personal information. The notice to affected individuals recommended that they remain vigilant and aware of the potential impersonation of themselves or the Organization, suggesting there is reason to believe the personal information could be mis-used.

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 (social insurance number), 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 or spear-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 an unknown actor who deliberately circumvented safeguards to access emails and may have exfiltrated personal information. The notice to affected individuals recommended that they remain vigilant and aware of the potential impersonation of themselves or the Organization, suggesting there is reason to believe the personal information could be mis-used. 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 email and telephone on July 16, 2021, in accordance with the Regulation. Additional affected individuals were notified by email on August 3, 2021. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner