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	Edward Jones (an Ontario Limited Partnership) (Edward Jones Canada) (Organization)
Decision number (file number)	P2021-ND-187 (File #017150)
Date notice received by OIPC	August 28, 2020
Date Organization last provided information	August 28, 2020
Date of decision	October 14, 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 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 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: • first and last name, • address, • postal code, • account number(s), • account type(s), and • market values of SEI investments as of November 17, 2017. 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 Thursday, July 23, 2020, the Organization received a notice from its service provider, SEI Investments Canada Company (SEI), about a security incident.

	• SEI informed the Organization that personal information in the custody of SEI's own service provider, M. J. Brunner, Inc. (Brunner) was affected by a ransomware attack. Brunner provides services to SEI in connection with optimizing the delivery of SEI's services. • The Organization reported that the attack on SEI's vendor systems occurred on May 17, 2020, when an unauthorized third party used malicious software to gain access to, encrypt and download, data from the vendor's corporate servers. • The Organization understands from SEI that, around June 9-12, 2020, the cybercriminals posted screenshots on the internet containing samples of the exfiltrated data as proof that it had obtained valid data from Brunner. • The posts were reviewed by Brunner and SEI at the time and there was no indication of any data of the Organization's clients in the screenshots. • On July 13, 2020, SEI learned that the attackers had publicly published the downloaded data on the dark web. • SEI obtained a copy of the published data and on July 17, 2020 determined that the Organization's client information was implicated and notified the Organization.
Affected individuals	The incident affected approximately 10,725 individuals of which 2,107 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	<u>SEI and Brunner:</u> • Took immediate steps to assess and investigate the incident, including shutting down the vendor's network, notifying the FBI and hiring external cybersecurity experts to assist with the investigation and recovery. • Identified suspicious activity and shut down its network in response. • Notified the FBI and hired an external cyber-security firm to assist in its investigation. • Contacted with a ransom demand in connection with the exfiltrated data. <u>The Organization, SEI and their vendor:</u> • Took immediate steps to conduct a detailed investigation. • Took steps to ensure that clients will be required to authenticate their identity using information that was not included in the published dataset. • Briefed financial advisors and customer service agents to help ensure that they watch for suspicious events that may arise from this incident. • Reported incident to the Investment Industry Regulatory Organization of Canada, the Office of the Privacy Commissioner

	of Canada, the Commission d'accès à l'information du Québec, and the Information & Privacy Commissioner for British Columbia. • Provided notice and a credit monitoring solution to affected individuals for a period of two years.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on August 28, 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.	In its report to my office, the Organization did not specifically identify the type of harm(s) that might result from this incident, but its notification to affected individuals said "The Company will provide notice and a credit monitoring solution to affected individuals for a period of two years" and "Please be alert to any requests for your personal information and take steps to verify the identity of the individual making the request if you have any doubt." In my view, a reasonable person would consider that contact and financial information at issue could be used to cause the significant harms of fraud and identity theft.
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.	In its report to my office, the Organization did not specifically provide its assessment of the likelihood that significant harm will result from the incident, but its notification to affected individuals said it does "…not believe that this incident has put your personal or financial well-being at risk. However, as a courtesy, we partnered with Equifax to provide its Complete Advantage identity theft protection product for two years at no charge to you." 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 a third party who also demanded a ransom payment. The Organization reported that the cybercriminal had already both accessed and stolen the personal information and published it on the dark web.
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 and financial information at issue could be used to cause the significant harms of fraud and identity theft. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party who also demanded a ransom payment. The Organization reported that the	

cybercriminal had already both accessed and stolen the personal information and published it on the dark web.

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 that affected individuals were notified by letter on August 28, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner