



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-206 (File #017829)
Date notice received by OIPC	July 29, 2020
Date Organization last provided information	July 29, 2020
Date of decision	October 18, 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 <i>Personal Information Protection Act</i> (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”	<p>The incident involved username and password. The Organization reported that “With the exception of confirming the existence of (an) ... account, the unauthorized party was not able to access any (...) personal information.”</p> <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
DESCRIPTION OF INCIDENT	
<input type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• On May 11, 2020, the Organization detected unusual attempts to access certain client information.• The Organization took steps to block access and to investigate.• The Organization determined that between March 30 and May 18, 2020, an unauthorized party leveraged client credentials, to access client account information.• The Organization reported it has no evidence that these usernames and passwords were obtained through its systems.

	<ul style="list-style-type: none"> The Organization reported that the attack merely confirmed that the credentials were valid, but did not otherwise provide access to any personal information of the affected individuals.
Affected individuals	The incident affected 64 individuals, including two (2) individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> Hired outside cybersecurity experts to investigate the incident. Blocked the unauthorized party from submitting requests to access servers and implemented a forced password change for all affected accounts. Offered identity theft protection to affected individuals. Recommended clients to change passwords to a new and unique password. Blocked the unauthorized party’s IP addresses from submitting requests to the Organization’s server. Implementing controls to reduce the risk of credential stuffing. Enhanced authentication procedures. Reported the incident to the Investment Industry Regulatory Organization of Canada and has also provided notice.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on July 10, 2020.

REAL RISK OF SIGNIFICANT HARM ANALYSIS

<p>Harm</p> <p>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.</p>	<p>In its report of the incident, the Organization did not specifically identify harms that might result from this incident but in its letter and notification to affected individuals, the Organization said:</p> <p style="text-align: center;"><i>We do 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 Premier identity theft protection product for two years at no charge to you.</i></p> <p>In my view, a reasonable person would consider that the credential information at issue could be used to cause the harms of identity theft and fraud, and to compromise other online accounts. These are significant harms.</p>
---	--

<p>Real Risk</p> <p>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.</p>	<p>In its report of the incident, the Organization did not specifically provide an assessment of the likelihood of significant harm resulting, but said “...the attack merely confirmed that the credentials were valid, but did not otherwise provide access to any personal information of the affected individuals”.</p> <p>In my view, a reasonable person would consider the risk of harm is increased as the incident was the result of a deliberate, credential</p>
---	--

	stuffing attack. The Organization reported that credentials were valid and could be used to access user accounts illegally and without authorization. The attacks appear to have been ongoing for approximately 6 weeks before the Organization discovered the threat.
--	--

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 credential information at issue could be used to cause the harms of identity theft and fraud, and to compromise other online accounts. These are significant harms. The risk of harm is increased as the incident was the result of a deliberate, credential stuffing attack. The Organization reported that credentials were valid and could be used to access user accounts illegally and without authorization. The attacks appear to have been ongoing for approximately 6 weeks before the Organization discovered the threat.

I require the Organization to notify the affected individuals whose 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 July 10, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner