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	Nicola Wealth Management Ltd. (Organization)
Decision number (file number)	P2020-ND-085 (File #015608)
Date notice received by OIPC	April 2, 2020
Date Organization last provided information	May 6, 2020
Date of decision	July 28, 2020
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 *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 for most of the affected individuals: • name, • email address, • date of birth, • age, • place of residence, • telephone number, • occupation, • name of spouse, • quantity of assets under management with Organization, • account numbers, and • the date on which the individual became a client of the Organization. For a subset of the affected individuals, the incident involved all or some of the following information: • social insurance number, • tax return, • net worth statement, and

	• will and testament. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 19, the Organization's CEO's assistant received a suspicious email purporting to be from the CEO directing her to pay an invoice. • The assistant confirmed with the CEO that the email in question was not legitimate. • The Organization discovered an unknown third party temporarily gained access to the CEO's email account through a webmail application, and potentially accessed, viewed or downloaded a number of emails over a period of approximately 11 hours. • The Organization found no evidence of compromise with respect to its server, devices or client portal.
Affected individuals	The incident affected 144 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Suspended the CEO's email account and removed the intruder's access to the webmail account. • Disabled webmail access. • Forced a global password reset for all employees of the Organization. • Reinforced recent security training with employees. • Developed a protocol to address the removal of non-essential sensitive personal information from internal reports. • Further refined its protocol for the secure transmission of documents containing sensitive personal information. • Further reinforced with employees the need to exercise caution to resist phishing and other malicious attempts. • Raised awareness with its clients that they should use the secure client portal to share documents with the Organization and refrain from emailing attachments with sensitive information (e.g. tax returns, wills and testaments). • Continuing to strengthen security infrastructure. • Provided affected individuals with a three year subscription for credit monitoring and identity theft services. • Notified the police of the incident. • Notified privacy regulatory authorities.

Steps taken to notify individuals of the incident	The Organization provided a preliminary notice to prospective clients on March 27, 2020 and notified most affected individuals by email and mail on April 7 and April 8, 2020. The Organization said contact information was being verified for some affected individuals who would then be notified.
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 did not specifically identify harm(s) that might result from this incident reporting that "…the compromised information for the significant majority of impacted individuals does not give rise to the risk of identity theft". The notice to affected individuals, however, said "As always, you should be vigilant with respect to the widespread risk of phishing attacks" and offered a subscription to a credit monitoring service. In my view, a reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, resulting in increased vulnerability to identity theft and fraud. These are all 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.	As noted above, the Organization reported that "…the compromised information for the significant majority of impacted individuals does not give rise to the risk of identity theft", but nonetheless provided direction for avoiding phishing attacks. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) by an unknown third party and it appears the unauthorized access to the email account was used to send fraudulent emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that the unauthorized party viewed, read, copied, or downloaded the affected individuals' personal information.
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, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing, resulting in increased vulnerability to identity theft and fraud. These are all significant harms.	

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) by an unknown third party and it appears the unauthorized access to the email account was used to send fraudulent emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that the unauthorized party viewed, read, copied, or downloaded the affected individuals' personal information.

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization provided a preliminary notice to prospective clients on March 27, 2020 and notified most affected individuals by email and mail on April 7 and April 8, 2020, but that contact information was being verified for some affected individuals who would then be notified.

The Organization is required to confirm to my Office in writing, within ten (10) days of the date of this decision, that those individuals whose contact information is being verified have been notified in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner