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	Ross Taylor Financial Corporation (Organization)
Decision number (file number)	P2021-ND-291 (File #019779)
Date notice received by OIPC	February 26, 2021
Date Organization last provided information	October 21, 2021
Date of decision	March 2, 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 operates in Alberta 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: • full name, • telephone number, • email address, • address, • Social Insurance Number, • date of birth, • account number, • banking information, • employment information, • license, • birth certificate, • passport information, and • signature. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 18, 2021, the Organization became aware of a ransomware attack on its computer system by cyber criminals. • The computer system was breached by criminals gaining access to the Organization's internal network. • On January 25, 2021, the Organization became aware that personal information had been taken and that the data stolen may be available online on the dark web.
Affected individuals	The incident affected 2 families residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged forensics firm to secure the server environment. • Took steps to guard against similar situation in the future. • Reviewed systems security. • Closed off ports on the server that were unnecessary and deleting/creating offline copies of personal information stored on the server. • Notified law enforcement agencies. • Reported the incident to the Privacy Commissioner of Canada, and companies the Organization worked with. • Offered one year of credit monitoring and reporting services at no cost to affected individuals.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and letter on January 26, 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, *Possible harms that may occur are identity theft, financial fraud, fianncial (sic) loss, email phishing, blackmail and/or negative effets (sic) on a credit record.* I agree with the Organization's assessment. A reasonable person would consider the contact, identity, financial and employment information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email addresses could be used for phishing, increasing 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 reported, "The likelihood that the harm will result is unlikely." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion, ransom attack). The cyber criminal stole personal information from the Organization and made it available 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 the contact, identity, financial and employment information at issue could be used to cause the harms of identity theft, fraud and financial loss. Email addresses could be used for phishing, increasing 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 third party (deliberate intrusion, ransom attack). The cyber criminal stole personal information from the Organization and made it available 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 the Organization notified affected individuals by email and letter on January 26, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner