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	FreeThink Capital Inc. (Organization)
Decision number (file number)	P2021-ND-186 (File #017689)
Date notice received by OIPC	July 20, 2021
Date Organization last provided information	July 20, 2021
Date of decision	October 12, 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 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: • name, • address, • date of birth, • email address, • social insurance number, • passport number, • photo of driver's license, and • personal trading account number. 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 or around July 15-16, 2020, an intruder broke into the Organization's office.

	• Some unopened mail was moved on the reception desk, all locked filing cabinets were forcibly opened, and some paperwork was removed. • The Organization does not believe that any of the mail or paperwork was taken. Other than small amounts of cash found in employee workstations, the only piece of office hardware stolen was an employee's laptop. • The Organization is confident that the laptop was not breached and it is confirmed to be off-line and "contained" by the Organization's cybersecurity vendor. • The Organization's computers were not accessed during the break-in.
Affected individuals	The incident affected 11 individuals, of which 10 are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Moved sensitive files to new locked filing drawers with key maintained by senior staff. • Changed employee's password. • Will conduct immediate audit of current hardcopy files. • Enforce the use of an alarm system on the office suite entrance. • Reviewing the property's security system. • Recommended individuals adopt enhanced monitoring of their privacy and security. • Provided risk reduction and mitigation resources to individuals.
Steps taken to notify individuals of the incident	The affected individuals were notified by email on July 17, 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.	The Organization reported "It is possible that the intruder could have recorded some of the identifying, or otherwise sensitive, information above and could attempt identity theft and other related fraudulent activities." In my view, a reasonable person would consider that the contact and identity information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' 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.	The Organization reported, *Based on the scene discovered and what was identified as being stolen (i.e. small amounts of cash and a laptop), it is probable that the intruder was searching work stations and locked storage for small items of tangible value. It appeared as though some paperwork was moved on desk surfaces and from locked drawers in order to search the general contents for items to steal. Most of the confidential files, including the majority of the individually identifying information above, did not appear to have been touched at all (i.e. was not removed from the opened filing drawers) and the unopened mail and paperwork that was moved appeared to be in piles that left no indication that the contents were reviewed.* *As discussed, the stolen laptop is confirmed not to have been breached and it will not be possible to breach it now that it has been contained by the organization's (security firm's) protection. The employee's password was considered to be exceptionally strong and in consideration of the outside chance that it was to come back online, the CISO has ensured that the device would only be able to communicate with (security firm).* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased, as it was the result of malicious intent (break-in). Although the Organization reported that "Most of the confidential files … did not appear to have been touched at all", I do not find this to be reassuring. The Organization can only speculate as to the actions and the motives of the thief.

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 and identity information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased, as it was the result of malicious intent (break-in). Although the Organization reported that "Most of the confidential files … did not appear to have been touched at all", I do not find this to be reassuring. The Organization can only speculate as to the actions and the motives of the thief.

I require the Organization to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individuals were notified by email on July 17, 2020. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner