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	Flexiti Financial Inc. (Organization)
Decision number (file number)	P2020-ND-054 (File #014799)
Date notice received by OIPC	January 21, 2020
Date Organization last provided information	January 21, 2020
Date of decision	May 22, 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 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: • name, • address, • email address, • date of birth, • social insurance number (if provided), • government issued identification information (if provided), • credit bureau information (for one of the individuals), • transaction information, • security questions and answers, • mother's maiden name, and • secret word. 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 December 28, 2019, the Organization received an email from someone purporting to be a hacker and claiming to have encrypted files, and deleted/encrypted backups. • The hacker demanded a ransom in exchange for the code to unlock the encrypted back up files, and also claimed to have stolen the Organization's database. The hacker threatened to release the information in unencrypted form if the ransom was not paid. • The Organization did not pay the ransom, but restored the database from a backup that was unknown to, and had not been accessed by, the hacker. • The incident occurred between December 19-28, 2019.
Affected individuals	The incident affected 7 individuals, of which 2 are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Investigated and took steps to block the unauthorized access. • Hired a third party forensics firm to assist with the investigation and confirmed that all unauthorized access had been blocked and no malware was present on systems. • Provided affected individuals with 12 months of free credit monitoring and identity theft insurance. • Provided "Additional Steps You Can Take to Protect Your Personal Information" in the notification to affected individuals. • Notified data protection authorities.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on January 22, 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 that "Given the nature of the information involved, it is possible that the impacted individuals may be at risk of identity theft or fraud." In my view, a reasonable person would consider the contact, credentials, identity and financial information at issue could be used to cause the significant harms of identity theft, and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud.

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 did not specifically assess the likelihood of harm resulting from this incident, but said: *Given the nature of the attack, the hacker's ransom demand and the results of our investigation, we believe that the purpose of the attack was to shut down [the Organization's] operations by deleting and encrypting [the] database so that [the Organization] would pay the ransom to get its business operational again. While some customer information was stolen, we believe that this customer information was stolen to bolster the hacker's ransom demand (i.e. to be able to show … evidence of data theft) and that data theft was not the primary purpose of the attack.* 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 an unknown third party (deliberate intrusion, ransom demand). In addition, personal information about seven (7) individuals was accessed and stolen.

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, credentials, identity and financial information at issue could be used to cause the significant harms of identity theft, and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud. 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 demand). In addition, personal information about seven (7) individuals was accessed and stolen.

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 verbally and by letter on January 22, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner