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	The Brenda Strafford Foundation Ltd. (the "Organization")
Decision number (file number)	P2019-ND-101 (File #012390)
Date notice received by OIPC	March 6, 2019
Date Organization last provided information	March 6, 2019
Date of decision	July 17, 2019
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 indicated that it is a non-profit organization as defined in PIPA, but did not clarify how it is incorporated or registered. To the extent that it qualifies as a non-profit as defined in PIPA, the Act applies to personal information that is collected, used or disclosed in connection with a commercial activity. The Organization reported that it "…provides Long Term Care and Supportive Living care to aged adults… and [employs] just over 1000 employees and all associated activities related to employing staff: Payroll, HR, Scheduling etc.". It appears that the information at issue was collected, used and/or disclosed in connection with commercial activities. To the extent this is the case, PIPA applies.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • date of birth, • residence, • telephone number, • pay and bank details (in encrypted SQL databases; the Organization reported there is no evidence that these were uploaded)

	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 February 5, 2019, a ransomware virus was introduced into the Organization's network. • The virus encrypted the main hosts, VMs and Primary backup store. • The virus was not detected and due to the nature of the virus, logs were also lost due to encryption. • The breach was discovered the same day due to performance changes to systems and detection of ransomware encryption notes.
Affected individuals	The incident affected approximately 1,800 individuals.
Steps taken to reduce risk of harm to individuals	• Removed the attack vector and remote access is now only possible via VPN. • Changed all administrator credentials and instructed staff to change their passwords. • Enhancing network security and implementing security improvements. • Notified all staff and residents and provided harm limitation advice.
Steps taken to notify individuals of the incident	Affected individuals were notified between February 11-15, 2019 by email and memos posted for residents or others potentially impacted.
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 "Access to personal identiable [sic] information and bank/payment details could result in financial harm to individuals/the organization." In my view, a reasonable person would consider that the contact and identity information at issue on its own, but particularly in conjunction with financial information, could be used to cause the significant harms of 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 reported: *Very low likelihood of harm to either staff or clients:* *BSF encrypted confidential data within the network with limited access (SQL databases).* *The attack agent was a ransomware virus commonly used to extract cryptocurrency from the victim and there is no evidence of any data being uploaded during the attack window.* *Servers and networks were disconnected on discovery of the attack - a short attack window.* *iON united has investigated the attack and determined that no information was posted on Dark Net sites about the attack or recovery of any data/credit cards etc.* In my view, a reasonable person would consider that 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 and ransomware). Although the Organization reported there is no evidence of data being uploaded, it also reported that logs were encrypted as a result of the virus. I understand this to mean that the Organization cannot be certain that malicious actors did not exfiltrate the personal information at issue.

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 on its own, but particularly in conjunction with financial information, could be used to cause the significant harms of 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 and ransomware). Although the Organization reported there is no evidence of data being uploaded, it also reported that logs were encrypted as a result of the virus. I understand this to mean that the Organization cannot be certain that malicious actors did not exfiltrate the personal information at issue.

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 individuals were notified between February 11-15, 2019 by email and memos posted for residents or others potentially impacted. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner