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	Edson Medical Centre
Decision number (file number)	P2021-ND-017 (File #016036)
Date notice received by OIPC	September 20, 2019
Date Organization last provided information	January 18, 2021
Date of decision	February 16, 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 the individuals 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 Organization reported the incident involved "emails/phone numbers/banking information". 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 September 5, 2019, the Organization discovered a former employee's email account had been accessed without authorization. • The breach was discovered when an employee from Scotiabank (Edson Branch) brought over paperwork to be signed, authorizing the transfer of funds to an unknown account to pay an overdue invoice. The bank had received the request to transfer the funds from the former employee's email account with the Organization.
Affected individuals	The Organization reported the incident affected five (5) Board Members.

Steps taken to reduce risk of harm to individuals	• Immediately shut down affected email accounts. • Reported the matter to the Scotiabank Fraud Department. • Confirmed that the former employee's access to the Organization's systems was deactivated when the employee left. • Audited previous emails to identify any other unauthorized activity and found no further issues. • Change passwords for email annually. • Provide privacy training to staff and reminders on a regular basis.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on September 5, 2019.
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 "Other individuals maybe [sic] contacted by this individual in an effort to acquire money". In my view, a reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, 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 that "There maybe [sic] a small chance that others may be contacted". In my view, a reasonable person would consider the likelihood of harm is increased because the breach is the result of deliberate, malicious action, and the perpetrators attempted a fraudulent financial transaction.
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 and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm is increased because the breach is the result of deliberate, malicious action, and the perpetrators attempted a fraudulent financial transaction. I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).	

I understand the Organization notified the affected individuals by letter on September 5, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner