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	RiverMend Health, LLC (Organization)
Decision number (file number)	P2019-ND-034 (File #007098)
Date notice received by OIPC	November 9, 2017
Date Organization last provided information	January 29, 2018
Date of decision	February 19, 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 the individual 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, addiction and treatment centre located in Atlanta, Georgia USA, and is an "organization" as defined in section 1(1)(i) of PIPA. The Organization is not a health custodian as defined in Alberta's *Health Information Act* (HIA), such that the HIA would apply in this matter.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • date of birth, • address, • Social Security Number, • diagnostic information, and • insurance information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization operates out of Atlanta, Georgia USA, and was unable to confirm where the personal information of the affected individual in Alberta was collected. To the extent the personal information was collected in Alberta, PIPA applies.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 10, 2017, the Organization identified suspicious emails being sent from an employee's account. • The Organization investigated and determined an unauthorized individual had gained access to the employee's email account beginning on or about July 27, 2017 and continuing until August 11, 2017. • The Organization has no evidence that any patient information was misused or specifically targeted.
Affected individuals	The incident affected one (1) Alberta resident.
Steps taken to reduce risk of harm to individuals	• Identified possible affected individuals and put in place resources to assist them. • Implemented additional safeguards to protect the security of information in its systems. • Established a hotline for affected individuals to contact with questions or concerns. • Providing guidance related to protecting against identity theft and fraud. • Reported the incident to state regulators.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified by letter sent on October 9, 2017.
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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals included a document called "*Steps You Can Take to Prevent Identity Theft and Fraud*." In my view, a reasonable person would consider that the contact, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. 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 did not specifically assess the likelihood that significant harm would result from this incident, but reported that it "currently has no evidence that any patient information was misused or specifically targeted." 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 into an employee's email account). The Organization said it has no evidence that the information was misused or specifically targeted; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for approximately two weeks.

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, identity and financial information at issue could be used to cause the harms of identity theft and fraud. Medical information could be used to cause the harms of hurt, humiliation and embarrassment. These are all 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 into an employee's email account). The Organization said it has no evidence that the information was misused or specifically targeted; however, the compromised information may well have continuing value over time. Further, the information may have been exposed for approximately two weeks.

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

I understand the Organization notified the affected individual by letter sent on October 9, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner