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	Field LLP (Organization)
Decision number (file number)	P2018-ND-011 (File #007295)
Date notice received by OIPC	December 5, 2017
Date Organization last provided information	December 20, 2017
Date of decision	January 10, 2018
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify this individual 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, • medical information, and • income tax information (may have included the social insurance number). This information is about an identifiable individual 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 April 18, 2017, the Organization learned that two binders of materials relating to a law suit fell out of the trunk of an employee's vehicle while in transport. • The Organization believes the materials fell out of the trunk on or about April 16, 2017.

	• The Organization was not aware this had occurred until contacted by the opposing legal counsel who reported that hard copy records of his client (the affected individual) had been located on the street by a third party. The third party returned the records to the affected individual's lawyer. • The Organization was not advised by the affected individual's counsel which records were located and returned to him. The Organization understands that records returned to him constituted all records that were initially lost, and stated it has no reason to believe otherwise; however, the Organization stated there is no way of knowing for certain that all the material lost was returned to the affected individual's counsel. • As far as the Organization is aware, the information was retrieved by a single third party. • The Organization's assessment of the breach at the time was that the incident did not rise to the level of a reportable breach under section 34.1 of the *Personal Information Protection Act* (PIPA) given the brief period of time between the loss of the records and the recovery, and the fact that the affected individual had full knowledge of the incident and legal counsel providing the affected individual with advice. • The Organization understands that the records were recovered without loss to the affected individual. • On or about November 21, 2017, the affected individual contacted the Organization's employee who was involved in this matter threatened to report the employee to her professional body unless payment was received. The affected individual did not claim any harm. • The Organization reassessed the breach, and their assessment remains substantially the same: the risk of harm to the affected individual is very low, but out of an abundance of caution, the organization decided to report the breach to the Office of the Information and Privacy Commissioner.
Affected individuals	The incident affected 1 resident of Alberta.
Steps taken to reduce risk of harm to individuals	The Organization reported that it is "…conducting an internal review of the policy for records handling (both electronic and hard copy) to ensure that in the future all records are transported by means that minimize the risk of any future privacy breaches. One means of better protecting hard copy records is to ensure they are transported in a locked container that cannot be accessed by any unauthorized third parties."
Steps taken to notify individuals of the incident	The affected third party was notified by her legal counsel. The Organization said it is "not aware specifically how she was notified."

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 "The type of harm that could result includes humiliation, fraud and identity theft" and "We assess the information is of a sensitive nature given that it includes the third party's medical records and SIN." I agree with the Organization. The contact and identity information could be used to cause the harms of identity theft and fraud. The medical information at issue could be used to cause the harms of hurt, humiliation, and embarassment. 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 "We assess a relatively minor to fair chance that a likelihood of harm could result. The records at issue are a single hard-copy. Our understanding is that an individual located the records, retrieved them and returned them to the third party or her legal counsel. We do not know specifically how long the information was exposed; however, we believe the incident occurred on April 16, 2017 and the records were retrieved no later than April 18, 2017 and subsequently returned to the third party or her legal counsel; meaning at most the information was exposed for 2 days. As far as we are aware, the information contained in the records related to only one individual and would be expected to affect only that one individual. The affected individual is not someone who would be considered a "vulnerable individual" … we are not aware of any instances where the information has been used for such purposes." In my view, a number of factors reduce the likelihood of harm resulting in this case, including that the incident resulted from human error and not malicious intent, the third party who found the records reported the breach to the affected individual's lawyer and there does not appear to be a personal/professional relationship between the affected individual and the third party. Nonetheless, and considering the sensitivity of the information at issue in this case, I am concerned that the Organization is not certain whether all of the information at issue was recovered and does not know for sure how long it was exposed, or whether or not it was copied, used, or viewed by other third parties. As well, the Organization does not know whether the affected individual received notification of the breach from her lawyer in accordance with section 19.1 of PIPA. Although the Organization is not aware of the personal information being used to cause harm at this time, this does not necessarily mitigate the potential harm from identity theft or other forms of fraud occurring in the future.

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 individual. The contact and identity information could be used to cause the harms of identity theft and fraud. The medical information at issue could be used to cause the harms of hurt, humiliation, and embarassment. These are significant harms. A number of factors reduce the likelihood of harm resulting in this case, including that the incident resulted from human error and not malicious intent, the third party who found the records reported the breach to the affected individual's lawyer and there does not appear to be a personal/professional relationship between the affected individual and the third party. Nonetheless, and considering the sensitivity of the information at issue in this case, I am concerned that the Organization is not certain whether all of the information at issue was recovered and does not know for sure how long it was exposed, or whether or not it was copied, used, or viewed by other third parties. As well, the Organization does not know whether the affected individual received notification of the breach from her lawyer in accordance with section 19.1 of PIPA. Although the Organization is not aware of the personal information being used to cause harm at this time, this does not necessarily mitigate the potential harm from identity theft or other forms of fraud occurring in the future. The Organization is required to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and confirm to my Office, within ten (10) days of the date of this decision, that this has been done.

Jill Clayton
Information and Privacy Commissioner