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	TGM Law (Organization)
Decision number (file number)	P2021-ND-240 (File #018780)
Date notice received by OIPC	October 19, 2020
Date Organization last provided information	August 17, 2021
Date of decision	November 30, 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 those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved electronic copies of court documents and family law based disclosure, including copies of identification and financial records. 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 October 7, 2020, the Organization's office was broken into. • The perpetrators stole a laptop, petty cash, and other physical items. • The laptop was linked to a cloud server. The Organization reported that "We have no indication the informaiton (sic) on this laptop has been accessed."
Affected individuals	The incident affected approximately 350 individuals whose information was collected in Alberta.

Steps taken to reduce risk of harm to individuals	Organization • Disabled the laptop access/connections to its office suite of products and cloud based systems. • Notified its bank who has been monitoring accounts for unusual activity. • Rekeyed the storage room and all office doors, desk drawers, filing cabinets, added deadbolts at office exits, changed passwords to computers, cloud servers, tracking unusual file activity, etc. • Considering additional alarms/cameras. • Will have a separate file room with lock to store any laptop purchased in future with the files. Landlord • Repaired the exterior door broken into and installed new lighting, locks on effected building entrances. • Will be installing cameras will be installed both inside and outside the building along with a new security entry system and alarms. • Contacted the RCMP.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone, email or in-person on October 16, 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 the harms that might result from this incident include "Breach of confidentiality, fraud, identity theft, are a remote possibility." In my view, a reasonable person would consider the contact, identity and financial information and legal information at issue could be used to cause the harms of identity theft, fraud and financial loss. Family law based disclosures could be used to cause hurt, humiliation or embarrassment. 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 its belief that it is …. *… unlikely any information will be accessed and that if it is that harm will result. The items stolen in our office and the building, generally were items of convenience, easy to pocket and easy to sell, the perpetrators did not take or attempt to take any physical files, papers, cheques or other "information" from our office. There was an opportunity to steal blank cheques and none were taken. Other businesses in the building had petty cash, access cards, food, etc. stolen. Only one filing cabinet was damaged which contained about a hundred dollars in petty cash. The laptop is password protected and all connnections*

	(sic) with cloud servers which contain the information were disabled, passwords changed within an hour or so of discovery. We are a small office with 3 computers, a hard drive hidden behind a tower was left behind and the desktops were not touched. Access to our adobe account was also disabled to prevent access to the files without passwords. All accounts are being monitored with email notification, daily observation, etc. You have to login into our adobe and microsoft (sic) account to access most everything. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in). The Organization can only speculate as to the motives of the thief. The laptop was password protected, but the Organization did not report that it was encrypted.

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, identity and financial information and legal information at issue could be used to cause the harms of identity theft, fraud and financial loss. Family law based disclosures could be used to cause hurt, humiliation or embarrassment. These are significant harms. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (break-in). The Organization can only speculate as to the motives of the thief. The laptop was password protected, but the Organization did not report that it was encrypted.

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 affected individuals were notified by telephone, email or in-person on October 16, 2020. The Organization is not required to notify the individuals again.

Jill Clayton
Information and Privacy Commissioner