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	Lyfe Kitchen Retail (Canada) Trust (Organization)
Decision number (file number)	P2015-ND-76 (File #001154)
Date notice received by OIPC	July 8, 2015
Date Organization last provided information	August 21, 2015
Date of decision	November 16, 2015
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 is a Trust formed in the province of Alberta, and qualifies as an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • Social Insurance Number (SIN), and • trust account number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On the evening of June 11, 2015 the Organization's Vancouver office was broken into and a laptop was stolen. The laptop was password protected but not encrypted. The theft was discovered the next morning. • The Organization had typically used this laptop to access a Dropbox web service. If the password was entered, a user could access a file containing the information at issue. • The Organization reported that the file was only stored on Dropbox and on a separate storage stick and not on the laptop; however, it could not confirm there was no temporary file stored on the laptop. • The laptop was not recovered.
Affected individuals	A total of 925 individuals were affected, including 172 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The incident was reported to the police. • Office locks were changed and all internal office doors are locked. • Laptops with files are now encrypted.
Steps taken to notify individuals of the incident	Individuals were notified by letter and/or email on July 6, 2015.
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 recognized the affected individuals may be at risk for identity theft. I agree with the Organization. The personal information involved is sensitive identity information. The information could be used to cause the harms of identity theft and fraud. In my view, 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 it considered there to be a low risk of harm to the affected individuals because there was no evidence of malicious intent, the suspect (who was on video tape) was known to police as someone who is likely to "wipe" the computer and try to sell it for quick money. The thief also left behind the power cord. In my view, the likelihood of harm resulting from this incident is increased because the personal information was stolen, which does indicate malicious intent. Further, the information has not been recovered. The laptop was password protected but not

	encrypted. The Organization is unable to confirm there were no temporary internet files accessible from the laptop.

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.

The personal information at issue could be used to cause the significant harms of identity theft and fraud. The personal information was stolen, indicating malicious intent. Further, the information has not been recovered. The laptop was password protected but not encrypted. Finally, temporary files may have been stored on the computer, which could allow access to a copy of the personal information saved to an online storage service.

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 email and/or letters dated July 6, 2015 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner